Performance Work Statement (PWS)

for the

VA Electronic Health Record Modernization System

ORIGINAL DATE: October 5, 2017
Final Version 2.1

AMENDMENT 01 DATE: November 7, 2017

AMENDMENT 02 DATE: November 20, 2017

AMENDMENT 03 DATE: February 16, 2018

AMENDMENT 04 DATE: May 7, 2018

Department of Veterans Affairs

Contents

1.0 BACKGROUND

This Performance Work Statement (PWS) establishes the requirements for Contractor-provided solutions in support of an enterprise-wide Department of Veterans Affairs (VA) Electronic Health Record (EHR). VA is replacing its current EHR, Veterans Information Systems and Technology Architecture (VistA) with a commercial EHR to modernize VA EHR processing and to promote interoperability of medical data between the Department of Defense (DoD), VA and community providers. When implemented, the EHR System will provide access to authoritative clinical data sources, and over time become the authoritative source of clinical data to support improved population health, patient safety, and quality of care provided by VA.

This contract was awarded after a determination by the Secretary of Veterans Affairs to be in the public interest under FAR 6.302-7. The goal of the accelerated award is to deliver a modernized system in the best interests of Veterans, their healthcare, and the providers that care for them both inside the VA and in commercial care settings.

This award contemplates the provision of services by Cerner Government Services, Inc. (Cerner), and accordingly the documents reference Cerner and its software and services. The VA may determine a different source of software and/or services will best serve the interests of Veterans for such services including quality of care, patient engagement, operational efficiency or interoperability to fulfill the goals of Electronic Health Record Modernization, the Veterans' Choice program, or other areas as the VA may decide. The VA may then follow the Federal Acquisition Regulations to seek other sources for the services.

The Contractor shall provide a total EHR solution including the following: program management, an enterprise-wide EHR system, change management, training, testing, deployment services, sustainment and other solutions encompassing the entire range of EHR requirements, to include but not be limited to hosting, software, and hardware incidental to the solution. Accordingly, Task Orders (TOs) may include acquisitions of software and information technology (IT) products as well as the services required to implement the EHR solution across VA. For purposes of this PWS, the VA EHR solution will be referred to as the VA Electronic Health Record Modernization system (EHRM). The EHRM solution shall focus priorities on the Veteran and clinician experiences.

EHRM is based on the electronic health record acquired by the Department of Defense known as the MHS GENESIS system, which is at its core, Cerner Millennium. The adoption of a single joint system between VA and DoD will allow all patient data to reside in a common system to have a seamless link between the DoD and VA. The DoD authorized system will be augmented to include additional functionality to meet VA requirements. Over time, the goal is the creation of an integrated inpatient and outpatient solution with software components that have been designed, integrated, maintained, and deployed with a design architecture that allows for access to and

sharing of common data, common user interface, common workflows, common business rules, and common security framework that supports end-to-end healthcare related clinical and business operations.

EHRM is not intended as a mechanism to solely purchase IT products. Such products may be purchased to the extent that those products are necessary to deliver the solution required. These services, as well as related IT products, may encompass the entire life-cycle of EHRM. Moreover, services and related products covered under this contract shall be global in reach and the Contractor must be prepared to provide services and deliverables worldwide.

This PWS provides general requirements. Specific requirements shall be defined in individual TOs. Functional and non-functional requirements are described in Section 5.0 and are not mutually exclusive for TO requirements. Requirements may fall within one specific functional or non-functional area but in many cases, the requirements will encompass and apply across and within multiple areas to provide the total life cycle solution.

In addition, VA and Contractor intend to collaborate to create innovations designed to strengthen and improve healthcare for all veterans and active service members, and to improve the productivity and user experience for VA system users.

2.0 Scope

The Contractor shall provide, host and deploy EHRM across the VA enterprise including the following areas: project management, change management, training, testing, deployment services, sustainment and other solutions encompassing the entire range of EHR requirements, to include hosting, software, and hardware incidental to the solution. The Contractor shall develop and maintain interfaces as required to meet EHRM solution requirements. The Contractor shall deploy EHRM to all VA Medical Centers (VAMCs), Outpatient Clinics and other approved users of VA EHR functionality. The Consolidated Mail Outpatient Pharmacies (CMOPs) will have access to the EHRM. The Contractor shall support the Veterans Health Administration (VHA) revenue cycle reporting, business intelligence, data analysis and new employee/continuing education training activities and system optimization. EHRM capabilities will also be deployed to Veteran Benefits Administration (VBA) facilities and/or to support other VA use cases as required.

3.0 Applicable Documents

The Contractor shall comply with the following applicable documents. Additional applicable documents may be listed in individual TOs. The Contractor shall comply with VA security, privacy and records management policies, directives, handbooks, and guidelines except where there is a conflict with DoD security, privacy and records management policies, directives, handbooks, and guidelines implemented in the MHS

Genesis environment, in which case, joint governance will provide guidance to the Contractor.

1. 44 U.S.C. § 3541, “Federal Information Security Management Act (FISMA) of 2002”
2. Federal Information Processing Standards (FIPS) Publication 140-2, “Security Requirements For Cryptographic Modules”
3. FIPS Pub 201-2, “Personal Identity Verification of Federal Employees and Contractors,” August 2013
4. FIPS Publication 199, “Standards for Security Categorization of Federal Information and Information Systems,” February 2004
5. FIPS Publication 200, “Minimum Security Requirements for Federal Information and Information Systems,” March 2006
6. 5 U.S.C. § 552a, as amended, “The Privacy Act of 1974”
7. Public Law 109-461, Veterans Benefits, Health Care, and Information Technology Act of 2006, title IX Information Security Matters
8. 10 U.S.C. § 2224, "Defense Information Assurance Program"
9. 42 U.S.C. § 2000d “Title VI of the Civil Rights Act of 1964”
10. VA Directive 0710, “Personnel Security and Suitability Program,” June 4, 2010
11. VA Handbook 6102 (Internet/Intranet Services), July 15, 2008 Health Insurance Portability and Accountability Act (HIPAA); 45 CFR Part 160, 162, and 164; Health Insurance Reform: Security Standards; Final Rule dated February 20, 2003
12. VHA Handbook 1605.05, Business Associate Agreements, July 22, 2014(http://www.va.gov/vhapublications/)
13. 36 C.F.R. Part 1194 “Electronic and Information Technology Accessibility Standards,” July 1, 2003
14. NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information systems and Organizations
15. Office of Management and Budget Circular A-130, “Managing Federal Information as a Strategic Resource”, July 28, 2016
16. Title 32 CFR 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”
17. NIST Special Publication 800-66 Revision 1: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
18. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. Section § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
19. VA Directive 6500, “Managing Information Security Risk: VA Information Security Program,” September 20, 2012
20. VA Handbook 6500, “Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,” March 10, 2015 (
21. VA Handbook 6500.2, “Management of Breaches Involving Sensitive Personal Information (SPI)”, July 28, 2016

22. VA Handbook 6500.3, “Assessment, Authorization, And Continuous Monitoring Of VA Information Systems,” February 3, 2014
23. VA Handbook 6500.8, “Information System Contingency Planning”, April 6, 2011 (http://www1.va.gov/vapubs/)
24. Office of Information and Technology (OI&T) ProPath Process Methodology (Transitioning to Process Asset Library (PAL) (reference process maps at http://www.va.gov/PROPATH/Maps.asp and templates at http://www.va.gov/PROPATH/Templates.asp).).
25. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, “Recommended Security Controls for Federal Information Systems and Organizations”
26. One-VA Technical Reference Model (TRM) (http://www.va.gov/trm/TRMHomePage.aspx)
27. Federal Segment Architecture Methodology (FSAM) v1.0, December 2008
28. VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment, October 15, 2014
29. VA Directive 6300, Records and Information Management, February 26, 2009
30. OMB Memorandum, “Transition to IPv6”, ”, September 28, 2010
31. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, October 26, 2015)
32. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 24, 2014
33. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
34. OMB Memorandum 05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 5, 2005
35. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011
36. NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008
37. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
38. NIST SP 800-157, Guidelines for Derived PIV Credentials, December 2014
39. NIST SP 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012
40. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014
41. VA Memorandum, VAIQ #7100147, Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12), April 29, 2011
42. VA Memorandum, VAIQ # 7011145, VA Identity Management Policy, June 28, 2010
43. IAM Identity Management Business Requirements Guidance document, May 2013,

44. OMB Memorandum M-08-05, “Implementation of Trusted Internet Connections (TIC), November 20, 2007
45. OMB Memorandum M-08-23, Securing the Federal Government’s Domain Name System Infrastructure, August 22, 2008
46. VA Memorandum, VAIQ #7497987, Compliance – Electronic Product Environmental Assessment Tool (EPEAT) – IT Electronic Equipment, August 11, 2014 (reference Document Libraries, EPEAT/Green Purchasing Section,
47. Office of Information Security (OIS) VAIQ #7424808 Memorandum, “Remote Access”, January 15, 2014,
48. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
49. VA Memorandum, “Implementation of Federal Personal Identity Verification (PIV) Credentials for Federal and Contractor Access to VA IT Systems”, (VAIQ# 7614373) July 9, 2015,
50. VA Memorandum “Mandatory Use of PIV Multifactor Authentication to VA Information System” (VAIQ#7613595), June30, 2015,
51. VA Memorandum “Mandatory Use of PIV Multifactor Authentication for Users with Elevated Privileges” (VAIQ#7613597), June30, 2015; (VAIQ#7613597), June30, 2015;
52. Veteran Focused Integration Process (VIP) Guide 2.0
53. “VIP Release Process Guide”, Version 1.4, May 2016,
54. “POLARIS User Guide”, Version 1.2, February 2016,
55. 38 U.S.C. 7301 (b): Functions of Veterans Health Administration
56. VHA Handbook 1907.01: Health Information Management and Health Records
57. Office of Management and Budget Circular A-123: Management responsibilities for internal controls in Federal Agencies
58. VA Memorandum, “Proper Use of Email and Other Messaging Services”, January 2, 2018
59. Health Data Interoperability Management Plan v 3.0: DoD/VA Interagency Program Office, September 14, 2016
60. Healthcare Information Interoperability Technical Package (I2TP) v 6.0: DoD/VA Interagency Program Office, March 15, 2017
61. Joint Interoperability Strategic Plan (JISP) v1.0: DoD/VA Interagency Program Office, September 30 2017
62. 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications: Final Rule - October 6, 2015
63. (http://docs.smarthealthit.org/)
64. (http://docs.smarthealthit.org/authorization/)
65. HL7.org Standards as delineated on www.hl7.org
66. VA Directive 6066, Protected Health Information (PHI) and Business Associate Agreements Management, dated September 2, 2014
67. 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications: Final Rule - October 6, 2015.
68. Fast Healthcare Interoperability Resources (FHIR) Draft Standard for Trial Use (DSTU) 2 (v1.0.2-7202)

69. Argonaut Data Query Implementation Guide Version 1.0.0
70. Argonaut Data Query Implementation Guide Server
71. SMART App Authorization Guide : http://docs.smarthealthit.org/authorization/
72. OpenID Connect Core 1.0 incorporating errata set 1
73. Consent2Share (C2S) FHIR Consent Profile Designed for C2S application and associated access control solutions
74. CDS Services v1.0 Draft
75. HL7.org Standards : www.hl7.org
76. Web Services Registry Web Service Interface Specification V3.1
77. Patient Discovery Web Service Interface Specification V2.0
78. Messaging Platform Specification V 3.0
79. Authorization Framework Specification V 3.0
80. Query for Documents Web Service Interface Specification V 3.0
81. Retrieve Documents Web Service Interface Specification V 3.0
82. Document Submission Production Web Service Interface Specification V 2.0
83. Query-Based Document Exchange Implementation Guide V 1.1
84. Technical Trust Policy V1.2
85. CommonWell Health Alliance Services Specification Version 2.9.1
86. Health Data Interoperability Management Plan v 3.0: DoD/VA Interagency Program Office, September 14, 2016.
87. Healthcare Information Interoperability Technical Package (I2TP) v 6.0: DoD/VA Interagency Program Office, March 15, 2017.
88. Joint Interoperability Strategic Plan (JISP) v1.0: DoD/VA Interagency Program Office, September 30 2017.

4.0 Performance Details

The Contractor shall provide and/or acquire the services, hardware, and software required by individual TOs pursuant to the general requirements specified below. TOs may be executed up to, and may extend no further than five years beyond, the last day of the ordering period.

4.1 Contract Type

This is an Indefinite Delivery/Indefinite Quantity (IDIQ) Single Award TO contract. Individual TOs shall be issued on a performance-based Firm Fixed Price basis.

4.2 Ordering Period

The total potential ordering period for this effort is ten years, consisting of a five-year base ordering period and one, five-year optional ordering period.

4.3 Hours Of Work

Hours of work shall be in accordance with (IAW) individual TO requirements.

4.4 Place Of Performance

The place of performance shall be identified in individual TOs. Locations in the Enterprise will be Government or non-Government sites within the continental United States (CONUS) and/or outside the continental United States (OCONUS) and set forth on Section D Attachment 005: List of Enterprise Sites. Locations may include but are not limited to Federal, State, or VA, data centers, facilities, regional offices, benefits delivery centers, medical treatment facilities, health clinics and community care facilities as defined in individual TOs.

4.5 Travel

Travel shall be IAW individual TO requirements. All travel shall be IAW the Federal Travel Regulations (FTR).

5.0 EHRM Function Areas

Individual TOs may encompass more than one task area listed below. Further task details are described to provide greater insight into the complexity and uniqueness of some potential TO requirements covered by this PWS. Task area requirements are not mutually exclusive and may apply across multiple functional areas and multiple task orders. Efforts to be performed by the Contractor under this contract are of such a nature that they may create a potential organizational conflict of interest as contemplated by Subpart 9.5 of the Federal Acquisition Regulation (FAR). Contractor personnel may be required to sign a non-disclosure agreement.

At some point in time, DoD and VA will establish joint governance over the shared environment containing MHS GENESIS and EHRM. Under joint governance, decisions pertaining to the shared environment will be reviewed and concurred by the joint governance entity. In the interim, VA shall be informed and consulted on all decisions impacting EHRM for VA review and concurrence.

5.1 Project Management

The Contractor shall provide EHRM Project Management, monitoring and analysis, strategy, enterprise architecture and planning support on an enterprise or individual task order level.

5.1.1 Project Management Support

The Contractor shall provide project management support to accomplish the administrative, managerial, logistical, integration and financial aspects specified in the overall program as well as in individual TOs. The Contractor shall identify an individual as the primary contact point for all project issues/concerns/status. The primary POC shall be empowered to make decisions and manage issue resolution across all

supporting legal entities comprising the EHRM solution. The Contractor shall support project management functions and reporting which include, but are not limited to:

a) Project Planning
b) Schedule Management
c) Site Deployment Tracking
d) Financial Management
e) Quality Management
f) Resource Management
g) Requirements Management
h) Communications Management
i) Project Change Management
j) Organizational Change Management
k) Risk Management
l) Configuration Management
m) Performance Management
n) Value Management
o) Knowledge Management
p) Governance
q) Security

5.1.2 **VIP Reporting**

In accordance with Major Program VIP Development Deployment Processes, the Contractor shall provide program development and deployment status and reporting to VA for VA documentation and support of VIP requirements.

5.1.3 **Strategy and Planning**

The Contractor shall provide services that facilitate strategic decisions for VA's implementation of EHRM. This includes conducting a systematic assessment of the enterprise VistA installation and supporting systems and processes in order to provide strategic recommendations on such key considerations as:

a) EHRM enterprise architecture and hosting
b) Deployment strategy
c) Site preparation requirements
d) Interface requirements
e) Compliance with applicable security requirements
f) Compliance with applicable Identity Access Management requirements
g) Network requirements
h) Additional hardware and software requirements
i) Data and workflows
j) Legacy systems and legacy data
k) Training and change management
l) Configuration management
m) Risk management

n) Performance metrics
o) Applicable governance requirements
p) Synchronization with DoD
q) Innovation strategy
r) Usability
s) Biomedical Devices
t) Interoperability: Health Information Exchange and Community Care

5.1.4 **Standards, Policy, Procedure and Process Development, and Implementation Support**

The Contractor shall provide support in the development and/or evaluation of new Standards, Policy Directives, Operating Procedures, Processes and/or assessments on their impacts when implemented.

5.1.5 **Requirements Development and Analysis Support**

The Contractor shall provide requirements development support as required by individual TOs. While the Contractor shall provide such support, the VA reserves the right to take the lead on coordinating input from the user and provider communities. VA may, at its discretion, incorporate analytics from other entities, and include them in its future Digital Veterans Platform, with which the EHR must interoperate using standards based APIs. Requirements support may include, but is not limited to:

a) Business and Application architecture
b) Business Process Reengineering
c) Requirements planning and management
d) Requirements gathering
e) Use Case development
f) Requirements analysis
g) Change management
h) Business Process Modeling and workflow management
i) Identification of site-specific requirements
j) Analytics and Business Intelligence
k) Innovation

5.1.6 **Technology Refresh and Configuration Reviews**

The Contractor shall perform technology refresh and configuration reviews to include any structure or process for realizing innovations that provides for business or technical changes. Technology refresh ensures new innovations are reviewed and adopted as required throughout the period of performance (PoP) of this contract.

5.1.7 **Data Management**

The Contractor shall support data aggregation, normalization, standardization and syndication.

The Contractor shall:

a) Perform an analysis of all data stored in VistA including historical data, interfaces, and paper records to determine data management requirements
b) Actively participate in joint governance for planning, strategy and tools for master-data management of VA data in the Contractor-provided solutions based on community and VA coordinated analytic algorithms.
c) Perform an analysis of data stored in other legacy systems in order to determine data migration approach and interface requirements if any.
d) Propose approaches for legacy data management and archiving
e) Propose a methodology for ingestion and syndication of data with other government agencies and affiliates.
f) Plan an approach to ensure operational integrity for CDW based enterprise solutions
g) Establish an analytic and reporting strategy that includes an analytic and reporting environment provisioned with data and reporting tools
h) Perform an analysis and propose terminology standards for DoD/VA data synchronization based on industry standards recognized by National Institutes of Health (NIH), Office of the National Coordinator for Health Information Technology (ONC), and others.
i) Conduct exploratory analytics to support policy development, knowledge discovery, and model creation.
j) Maintain backward compatibility of the EHRM solution in such way as to maintain the quality of the data, to ensure that, once captured, the VA has access to and computational use of the data regardless of the evolution of the EHRM or age of the data.
k) Identify data quality issues found in data sourced from systems beyond its operational remit, applying the same validations and quality standards to incoming external data that it performs for data originated natively within the EHRM solution. Where the principle of seamless care requires that EHRM accept data that does not meet its internal data quality standards, Contractor shall implement the solution so that any incoming data that does not meet EHRM data quality standards shall be clearly flagged as such, and provide both process and user interface to allow incorrect or missing data to be remedied if possible.

5.1.8 **Data Migration Planning**

The Contractor shall support data migration planning to support seamless care and to ensure operational integrity.

The Contractor shall:

a) Develop a Data Migration Plan (DMP) that provides an understanding of the EHRM Solution implementation sequence and priorities, data quality, data volumes, and data extract, transformation and load strategy for both the EHRM and Population Health Management solutions.
    i. The DMP shall describe the approach for data ingestion and extraction, storage, access, data conversion, and data security strategies.
    ii. The DMP shall account for key clinical data in VistA along with other relevant systems and outline a strategy to make that viewable and actionable.
    iii. The DMP shall also address data validation assessing the migration of VistA legacy data to HealtheIntent and Millennium.
    iv. The DMP should address how to migrate data that is still actionable and to maintain actionability
    v. The DMP shall identify, clarify, and propose approaches for the following:
        1. Data Integration (Data flow from VA to Cerner)
        2. Data Continuity (VA Legacy Data Integration)
        3. Data Syndication (Data flow from Cerner to VA and partner applications and databases)
b) Plan and document the data ingestion mechanism and processes along with terminology mapping to standards associated with data migration and data synchronization/syndication.
c) Plan initial and incremental loading of data into HealtheIntent to include batch and streaming (i.e. near real-time) options
d) Analyze and propose way forward for the capability for external apps to use HealtheIntent as a data source
e) Organize and facilitate a Joint VA/DoD/Cerner Data Governance Board to develop strategy and priorities.

Contractor and VA to create a strategy to establish an archival instance of a VistA instance once the site has migrated to Milleniuum and the local VistA instance is no longer being updated. This instance will be accessible and can be used for high latency extraction.

5.1.9 **Implementation Planning**

The Contractor shall:
a) Deliver an Implementation Plan that defines the Contractor's plan for deployment, training, change management, and sustainment of EHRM to the VA Enterprise
b) Brief VA EHRM management on, at a minimum, the following information:
    i. Enterprise deployment strategy
    ii. Change management approach
        a. EHRM System User Role definitions
        b. The availability of EHRM User Provisioning workflows
        c. Level of Effort estimate to provision all EHRM users during migration

d. Level of Effort estimate to provision new users and maintain end user permissions post migration

iii. Training approach

iv. Sustainment and helpdesk approach

c) Propose recommended change management activities for the most efficient and effective change management support of EHRM in the Monthly Progress Report
   i. Execute such activities upon Government approval
d) Participate in VA EHRM business process reengineering discussions and advise or present industry leading practices, processes and workflow
e) Conduct a comparative analysis between the EHRM solution-inherent workflows and the “As-Is” organizational business processes and provide recommendations on process re-engineering, change management and product configuration
f) Provide Business Process Workflow Diagrams and Role Definitions that define business and clinical workflows and describe how improved functionality and efficiency has been achieved, and establish EHRM System user role definitions
g) Provide a Role Assignment Identification Document that maps user roles, rights and permissions to EHRM roles

5.1.10 **Configuration Management**

The Contractor shall draft a Configuration Management (CM) Plan for review and comment by the EHRM Program Management Office (PMO). After mutual agreement on the plan, the Contractor shall adhere to the CM policies and practices as described in the Plan. CM includes supporting the definition of Configuration Items (CIs) and relevant attributes and relationships to manage, establishing procedures for change and controlling request for change, providing the status of the CIs, and auditing the actual and authorized versions of each item. Maintaining a complete and accurate CM system ensures the integrity of system/software baselines and designated CIs required to provide services.

5.1.11 **Value and Performance Management Reporting**

The Contractor shall propose and monitor value objectives for improved outcomes and continuous performance improvement throughout the PoP of this contract. The Contractor shall:

a) assist with data analysis to identify possible optimization projects to further drive performance excellence after implementation at each site.
b) work with VA leadership to establish future value objectives through strategic planning sessions.
c) incorporate change management, workflow and process review and data analytics using the change management methodology agreed by Contractor and VA with consistent recognition and promotion of value achieved.

The Contractor shall use a value realization framework and tools to assist VA with creating value metrics aligned with VA, VHA and clinical strategic goals, and targeted to EHRM and specify goals and Critical Success Factors (CSFs). Value metrics will include Key Results Indicators (KRIs), Key Performance Indicators (KPIs), and traditional Performance Indicators (PIs). The Contractor shall develop and implement tracking mechanisms to measure and report EHRM progress against clinical and business goals.

Clinical goals may include:

a) Patient experience
b) Clinical staff experience
c) Clinical Efficiency
d) Operational Efficiency
e) Safety and Quality (Better Health, Better Care)
f) Patient Engagement
g) Best Practices Adoption
h) Financial Outcomes
i) Access to Care
j) Community Care
    i. Health Plan Operations
    ii. Seamless Care
    iii. Access to Care
    iv. Choice
k) Population Health

Business goals may include:

a) Cost
b) Scope
c) Schedule
d) Security
e) Quality
f) Technical Performance
g) Patient Access to Care

The Contractor shall develop standards for VA approval to be used as input for VA determination of successful site deployment. These standards may be related to the Clinical and business goals, including user adoption rates, process adherence, training competency test results, patient throughput or other similar indicators of success. For system performance (example: availability, accuracy, efficiency) the Contractor shall propose any deviation from or changes to the metrics jointly agreed with VA that will need to be approved as success criteria. The ability to measure these clinical and business requirements shall be documented in a monitoring and reporting plan and measured and reported to VA throughout the PoP. These tracking mechanisms will evolve over time throughout the PoP of this contract as deployments advance across

the enterprise and the data available to support metrics expands.

5.2 EHRM SYSTEM

The Contractor shall provide an operational managed services solution for EHRM applications (software and subscriptions), application services and all supporting third party content required to deliver the functional and non-functional requirements set forth in the Requirements Traceability Matrix (RTM) included in Section D, Attachments 002 and 003 to this document.

5.2.1 Electronic Health Record Application

EHRM requirements are established at a strategic level and will guide the configuration and implementation of the system across VA. In addition to the requirements in the Government RTM, the Government may place orders for product enhancements or improvements to meet emerging needs, activate existing, but dormant capabilities in EHRM, or to address a need in the overall EHRM solution not explicitly extrapolated into the Government RTM.

EHRM is expected to unify and increase accessibility of integrated, evidenced-based healthcare delivery and decision-making. EHRM will support the availability of longitudinal medical records for the patients currently enrolled in the VA EHR and new patients as they transition into EHRM as set forth in the VA Enterprise as defined in section H1. EHRM will enable the application of standardized workflows, integrated healthcare delivery, and data standards for improved and secure electronic exchange of medical and patient data between the VA and its external partners, including the DoD, and other Federal and private sector healthcare providers. The workflows inherent to EHRM will be configured, adopted by and standardized throughout VA as applicable. EHRM will leverage data exchange capabilities in alignment with the Interagency Program Office (IPO) for standards-based health data interoperability and secure information sharing with external partners. Testing conducted under the Test and Evaluation Program Plan may include specific workflows to inform a demonstration of end-to-end clinical use cases involving external stakeholders.

5.2.1.1 Software Requirements

The Contractor shall:

a) Provide all applicable software licenses in accordance with all clauses, identifications and assertions, terms, and conditions related to commercial and non-commercial technical data, computer software, and computer software documentation to support the configuration, integration, custom development, test, software management, training, deployment, and end-user usage of EHRM
b) Manage and track all software licenses required to establish, operate, and maintain EHRM.

c) Provide initial limited licensing for Multum testing and integration with VistA
d) Maximize utilization of VA-provided enterprise licenses where available and appropriate.
e) Provide and update an EHRM Enterprise Release Schedule identifying:
    i. Software release packages based on security and system incidents
    ii. Planned Technology Refresh and Modernization activities
    iii. New installations and service upgrades
f) Identify and report issues and risk associated with software and report risks/issues and status of any mitigation actions in the Monthly Progress Report and at Program Management Reviews (PMRs), technical reviews, program milestones and configuration audits.
g) Configure workflows inherent to HealtheIntent for adoption throughout VA as applicable
h) Provide the ability to segregate information (e.g. from users, from DoD, separate practices for military sexual trauma (MST), employee health, and others)
i) Provide the ability to exclude/segregate/de-identify data from specific practices from HealtheIntent, e.g., MST.
j) The EHRM solution shall support broad access via tablet or mobile devices and pursue technology to reduce the burden to the clinicians. Platform specifics shall be adjudicated by joint governance and incorporated by VA at a TO level.
k) The EHRM solution shall provide third-party provider access to information using light-weight portals and support for future generation mobile devices.

5.2.1.2 **Hardware Requirements**

The Contractor shall provide and maintain Cerner-specific hardware required for the EHRM solution. This hardware includes such items as connectivity engines and device adaptors.

5.2.2 **Additional EHRM Functionality**

VA's requirements will evolve over the course of the IDIQ. To maximize meeting of government requirements while minimizing risk to the Contractor and VA, the parties will engage in periodic future-capability planning cycles. Future requirements may include such items as clinician access to EHRM via tablet.

The Contractor shall meet with the VA once a year to provide visibility to Contractor's roadmap of future capabilities. The Contractor's roadmap shall detail capabilities that the Contractor is anticipating to develop as part of its generally available (GA) product over one, two, and three years. The VA may request such capabilities in a manner that corresponds with wave task orders As mutually agreed between the Contractor and VA, the Contractor may host an interim capability planning event upon request. These interim planning events are expected to focus on wave task orders in the subsequent 12 months or to make adjustment to future milestones based on unforeseen information or events.

The Contractor shall include VA in all user groups and other planning activities that other major clients participate in and that are used to inform the prioritization of the Contractors development backlog. In addition, VA will provide input to applicable Cerner business units on capability prioritization.

The Contractor shall provide VA the right to acquire additional modules developed to support the evolving electronic health record commercial baseline throughout the PoP of this contract.

5.2.3 **Software Maintenance**

The Contractor shall provide its commercial support and maintenance services described in its End User License Agreement. Leveraging Contractor's best practices and agreed upon upgrade schedule between DoD and VA, software maintenance includes all releases of the software such as major releases, minor releases, maintenance releases. Maintenance will be conducted in such a way to minimize impact to the user community.

Contractor shall:

a) Maintain EHRM software including any Off the Shelf software applications and tools included in the solution
    i. Notify the Government of any software that is within two years of end of life, end of service, or end of Software maintenance release
    ii. Ensure all software has continuous vendor support
b) Renew software licensing and maintenance agreements as required throughout the PoP of the TO.
c) Support other functional dependencies, such as device certificates and PKI, if applicable
d)

5.3 **EHRM HOSTING AND MANAGED SERVICES**

The Contractor shall provide enterprise datacenter hosting and services consistent with the hosting requirements set forth in Contractor's Hosting Agreement. If a cloud hosting environment becomes a more viable solution over the Period of Performance, Cerner may migrate the joint DoD/VA hosting environment to a Cerner private cloud or external third party cloud upon concurrence and security validation from the joint DoD/VA governance authority. The Contractor shall:

a) Provide hosting and managed services to support delivery of the EHRM
b) As a minimum, employ appropriately tailored security controls from the high baseline of security controls defined in NIST Special Publication 800-53 and must ensure that the minimum assurance requirements associated with the high baseline are satisfied. The hosting environment shall be compliant with FISMA-

High or equivalent or higher controls. Any deviation from high impact controls must be approved by the Authorizing Official or designee.

c) Provide a primary and alternate data center to support continuity of operations and disaster recovery requirements
d) Support VA Network connectivity requirements
e) Provide all hardware, software, and services necessary to perform sustainment of EHRM in Contractor's hosted environment
f) Provide continuous technical support and system monitoring to immediately react to a system event
g) Utilize established commercial and proprietary automated tools to monitor and managed vital datacenter infrastructure and EHRM systems.
h) Administer support access by contractor personnel to the EHRM environment using two factor authentication via RSA SecurID in lieu of CAC/PIV authentication for managing solutions within the accredited boundary
    i. Access to the EHRM environment by administrative personnel external of the Cerner hosted network will be provided through a VDI and utilize appropriate CAC/PIV authentication
    ii. Administrators shall use non-privileged accounts, or roles, when accessing other system functions such as email, and if feasible, audit any use of privileged accounts, or roles, for such functions.
i) Support VA troubleshooting for network latency and packet loss issues to assist in identification of sources of network transport response time issues.
j) Leveraging Contractor's best practices and agreed upon upgrade schedule between DoD and VA, hosting maintenance includes patches, cybersecurity, and software assurance updates. Maintenance will be conducted in such a way to minimize impact to the user community.

5.3.1 **Non-Production Environments / Domains**

The Contractor shall:

a) Host and operate all EHRM non-production environments/domains that are functionally equivalent to production environments/domain. The environment/domains will support the non-production requirements and needs across the lifecycle of the VA EHRM, including development, testing, training, certification (for upgrades), and sustainment. Development activities include the activities to develop/build the interfaces between the EHRM, VistA, other VA systems and non-VA systems within the EHRM program scope. Test activities will be executed in these non-production environment that represent architecturally, operationally and technically similar non-production environments so that test and training results are identical as if run in production.

b) Work closely with VA to identify the number and use of non-production environment/domains required to mitigate the risk of development/test events schedule collisions or usage issues/conflicts between Contractor, VA EHRM and

DoD MHS GENESIS teams performing work in the same non-production environment/domain.

c) Work closely with VA EHRM and DoD MHS GENESIS teams to create/maintain a Non-Production Domain Integrated Master Tracking/Schedule of key activities taking place in non-production environments/domains to mitigate risks/issues impacting EHRM schedules. Risks/Issues may arise due to multiple teams sharing the domain environment.
d) Coordinate new requirements and modifications that impact the existing DoD-VA Joint Test Environments thru the DoD-VA Joint Test Environment workgroup.
e) Work jointly with VA and DoD MHS GENESIS teams as needed to establish network connectivity between non-production environments/domains and use established connectivity processes such as, VA ESCCB and DoD MHS GENESIS PEO change control for non-production environments.
f) Participate with VA in environment/domain network connectivity test to ensure the environments pass connectivity tests
g) Ensure EHRM system installed within the non-production environment/domain are functional
h) Participate with DoD MHS GENESIS/VA teams in environment/domain smoke tests as needed to ensure any DoD interfaces (like Joint Legacy Viewer or DoD DEERS) are functional (pass smoke tests)
i) Provide Access to non-production environments for VA (both VA government and VA contractors) resources involved in VA Test & Evaluation, as needed. Access type may vary. For example, some users will need access commensurate with their roles as trainers while others may need the same access they have in the production environment. Functional integration testers will need to change testing roles.
j) Use a non-production environment/domain to support VA Mockups of the medical operational environment (aka sim labs/learning centers) in which end users will interact with EHRM potentially to be used for training and other end user engagement activities.
k) Work closely with VA EHRM resources to determine the data requirements within non-production/domains in support of the VA mockup environment and the facility/site data that the medical devices in the VA mockup operational environment will be set up against.
l) Create, maintain, and provide the architecture/system diagrams showing how each non-production/domain environment is interfaced to VA systems with input from VA for the EHRM and VA systems integration.

VA will provide the non-production development/test environments for interface/integration development and test to VA's VistA and VA legacy systems. Contractor resources performing development and testing of VA Systems Interfaces will require VA network access depending on the location of development/testing environments/domains.

The medical device and peripherals configuration within the non-production environment/domain that supports the VA Mockup operational environment will be executed by the contractor upon VA request.

5.3.2 Continuity of Operations (COOP), Disaster Recovery (DR), and Business Continuity Planning Services

Disaster Recovery encompasses the policies and procedures to prepare for recovery of technology infrastructure and business operations critical to an organization after a natural or human-induced disaster to partially or completely restore services and critical functions within a predetermined time after a disaster or extended disruption.

The Contractor shall develop, maintain and update a Disaster Recovery Plan (DRP) (data center) level contingency plan which shall include a Policy Statement and a Crisis Communications plan proposed by the Contractor. The plan will be signed jointly by VA and DoD, and the Contractor shall facilitate a governance board which includes membership from all three organizations.

The Contractor shall:

a) Design, install, operate, and maintain COOP capabilities to enable plans for emergency response and supporting infrastructure (e.g., storage and backup operations, off-site storage) for post-DR of information systems
b) Develop system and network designs that enable EHRM services and network operations to survive individual component failure
c) Provide input to the Government for making system performance decisions in the event of a disaster or incident
d) Provide input to the Government After Action Reports (AAR) and lessons learned following exercises
e) Execute emergency failover COOP requirements
f) Support annual exercises of the DRP

The Contractor shall provide 724 Downtime Viewer read-only system to replace each of the over 170 instances of VistA Read-Only installations. This replacement shall be implemented as part of each site deployment.

The Contractor shall provide a back-up solution that includes a feed of EHRM data to an off-site location. The back-up system or equivalent off-line data source shall be subject to governance approval. The feed shall be encrypted in transit to the storage location. Cerner shall be responsible for transmitting the data to the VA-Cerner demarcation boundary. Data stored will be encrypted in accordance with the standards of the PWS. The Contractor shall provide VA access to the encryption keys.

5.3.3 System Quality and Performance Measures and Monitoring

The Contractor shall provide its commercial performance measurement system for system acceptance for discussion and review with VA. The Contractor shall conduct analysis and design activities for system quality and performance. The Contractor shall provide performance and availability trend analysis and supporting data in the Monthly Progress Report to show prediction, trending, and monitoring of system's performance trends. The Contractor is responsible for reporting all issues or errors associated with the EHR solution, and acknowledges and agrees that software errors creating patient safety risks shall not be considered confidential, proprietary or trade secrets, and accordingly, shall be releasable to VA or its agents. The VA retains the right to share any issue, error or resolution approach related to software errors creating patient safety risks.

5.3.4 Virtual Training Environment

The Contractor shall:

a) Install, integrate and maintain the Virtual Training Environment (VTE) and provide scenario-based training simulations with de-identified or synthetic data.
b) Provide access to the VTE as required for EHRM end-user training to meet deployment timetables.
c) Ensure that the VTE provides the following utilities/requirements:
    i. Environments used for training shall meet requirements specified in section 5.3.1, above.
    ii. Accessible locally or via a secure tunnel on the internet using desktops or laptops
    iii. Accessible from Government networks
    iv. Accessible by VA government and VA contractor users (upon signing of an NDA)
    v. Scalable to support up to 15,000 concurrent virtual users

5.3.5 Solution-specific Hardware and Hardware Maintenance

The Contractor shall:

a) Maintain EHRM System Contractor-provided hardware
b) Renew and manage EHRM system hardware maintenance agreements as required
c) Provide the necessary supply support (e.g., hardware spares, cabling, and test equipment) required for the repair of failed EHRM system components as described in End User License Agreement
d) Maintain all EHRM hardware components in compliance with manufacturers' warranties
e) As required, de-install, move, and install EHRM System computer hardware, excluding medical devices, in a manner that will not void warranties

f) Support hardware items once the commercial product warranties expire without voiding Return to Factory (RTF) warranties

5.3.6 Hosting of Legacy Data

5.3.6.1 Image Hosting

To support the transition to the EHRM Vendor Neutral Archive (VNA) for imaging, the Contractor shall migrate all DICOM and non-DICOM images from each VISN or site into the EHRM VNA at the time of deployment to each VISN or site.

To support the transition to the EHRM Vendor Neutral Archive (VNA) for imaging, the Contractor shall:

a) Migrate all DICOM and non-DICOM images and image artifacts from each VISN or site VistA Imaging Tier II storage system (NetApp Storage Grid) into the EHRM VNA prior to the time of deployment to each VISN or site.
b) EHRM generated images shall be made available to be viewed at VistA sites via industry standard integration with the Central VistA Imaging Exchange.

5.3.6.2 Legacy System Hosting

The Contractor shall provide infrastructure hosting services to support the Data Migration Plan (DMP) with the following alternatives:

a) Host a Mirrored copy of the VX130 extract to facilitate Data Migration into the HealtheIntent platform.
b) Host one or more VistA shadow instances as a ‘read-only’ archive of the legacy data.

5.4 Information System Authorization, Testing And Continuous Monitoring

The Contractor shall adhere to all applicable FISMA, FIPS, and NIST standards related to information system authorization, testing and continuous monitoring.

The Contractor shall meet agency Risk Management Framework (RMF) requirements (NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information System) for the maintenance of Authority-to-Operate (ATO). The commercial off-the-shelf (COTS) Electronic Heath Record (EHR) (Cerner Millennium) system hosted by Cerner Corporation is the Defense Health Agency (DHA) Enterprise Mission Assurance Support Service (eMASS) registered system (MHS GENESIS) and the IPO recognized authorization boundary. Changes to the system must be reported through the appropriate change control board with a Security Impact Analysis (SIA) conducted to determine if the changes constitute a significant change requiring re-authorization. If re-authorization is required as determined by the SIA, the Contractor

shall adhere to the information system authorization, testing, and continuous monitoring activities as defined by NIST. The appropriate government official will be notified in the event that a significant change as defined by the SIA will occur.

The Contractor shall provide and maintain the ATOs IAW the guidance provided in VA Directive and Handbook 6500, “Information Security Program”, VA Handbook 6500.3, “Assessment, Authorization, and Continuous Monitoring of VA Information Systems,” February 3, 2014, using a Governance Risk and Compliance (GRC) tool. Cerner shall maintain ATOs for all systems and devices managed by Cerner, including those residing in VA facilities.

The Contractor shall adhere to cybersecurity security and privacy controls (NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations) for the DoD/VA EHR authorization boundary, which are based on the security categorization (FIPS 199) currently designated by VA at the High impact level. Additionally, maintain the Defense Health Management Systems Modernization (DHMSM) Security Control Assessor (SCA) artifact templates, security checklists, assessment tools, and scripts used to complete the assessment and report for the Authorization Official (AO).

The Contractor shall support the DoD/VA ATO reciprocity process to minimize redundancy and meet cybersecurity compliance requirements by fully integrating VA into the continuous monitoring (NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organization) mechanisms required by the AO. The Contractor shall adhere to the following DoD (VA recognized) cybersecurity activities to be executed during the lifecycle of the program:

a) Cybersecurity posture determination based on Contractor provided scans and Independent government testing, including cooperative vulnerability and adversarial penetration testing.
b) Define milestones for validating the system posture and identifying potential vulnerabilities that would hinder the system receiving an ATO.
c) Continuous verification and validation of the cybersecurity controls to verify appropriate administrative, technical, and physical safeguards to protect all Government data, ensuring the confidentiality, integrity, and availability of Government data.
d) Continuous monitoring and verifying the documentation for all vulnerabilities in POA&Ms, with timelines, and mitigation strategies of findings.

5.5 **VA Enterprise EHRM Baseline Preparation**

The Contractor shall conduct pre-deployment system assessment and update activities required to accommodate an enterprise-wide EHRM deployment.

5.5.1 **Workflow Development and Normalization**

The Contractor shall support workflow normalization. The Contractor shall:

a) Configure new workflows to meet VA-specific requirements as appropriate under direction of EHRM Chief Medical Officer.
b) Identify and document gaps and recommendations for workflow differences
    i. Between locations of VA implementations
    ii. Between DoD and VA
    iii. Between each specialty/department
c) Propose and implement a methodology for continued synchronization of workflows internally to VA and between DoD and VA.
d) Participate in joint governance and change control
e) Support robust semantic modeling for the information associated with those workflows. The VA and its agents shall have unlimited rights to all models and algorithms developed by Contractor at VA expense and direction pursuant to a task order.
f) Support modeling and storage of data associated with workflows, which modeling shall be based on analytical algorithms and data models (1) developed by the Contractor, (2) co-developed by the Contractor in coordination with the VA health organizations and the community, (3) developed by VA health organizations, or (4) provided by third-party developers. The VA and its agents shall have unlimited rights to all algorithms and logic models developed by Contractor at VA expense and direction pursuant to a task order and incorporated in the EHRM solution.
g) Encapsulate workflows into platform-independent, standards-based, modeled clinical processes and pathways.
h) Provide content management oversight as well as tools to generate and curate workflow data.
i) If applicable, provide a traceability matrix of the RTM functional requirements to EHRM enterprise workflows.
j) The Contractor shall enable configuration of the application that supports external community data without requiring the clinician to go to special screens to see and use reconciled external data. By IOC entry, the Contractor shall support incorporation of the following external community data domains, including but not limited to these domains and sub-domains:
    - Problems
    - Allergies
    - Home Medications
    - Procedures - including associated reports and with appropriately filtered CPT codes
    - Immunizations
    - Discharge Summaries
    - Progress Notes
    - Consult Notes
    - History & Physicals

- Operative Notes
- Radiology and Diagnostic Reports (Into “Documentation” component)

By IOC exit, the Contractor shall support incorporation of the following external community data domains, including but not limited to these domains and sub-domains:

- Results
  - Labs
    - General
    - Pathology and Microbiology
  - Vitals
- Radiology and Diagnostic Reports (Into “Diagnostic Report” component)
- Images

k) Provide the VA with an understanding of how all workflows will impact VA care coordination and management processes (e.g., incorporating community information) to improve Veteran-centric delivery.

l) Within 36 months of the IDIQ award, provider workflows will be optimized to leverage discreet data domains listed in Section 5.5.1 j) using Clinical Decision Support hooks (CDS hooks) or other techniques to reduce clinician burden.

5.5.2 **Identity and Access Management**

The Contractor shall support VA Identity and Access Management requirements. It is anticipated the Contractor shall support sufficient identity and access management methodologies to support the integrity and security of initial deployments with additional more complex features added in a phased approach.

VA currently utilizes an enterprise Identity Management Service called Master Veteran Index (MVI). VA and DoD intend to collaborate to provide a single identity service. It is intended that this single service will become the identity integration point for the joint VA/DOD EHR. When developed, the Contractor shall connect to the single VA/DOD service. VA will notify Cerner of the single service status within 30 days of contract award for joint assessment of the way forward. In the case that the single service will not be available in time to meet the go-live date of the IOC site, the Contractor shall be required to support identity through MVI.

The VA currently utilizes a combination of access controls to protect health care information. As we move forward with a joint VA/DoD EHR system we will likely discover many types of access controls that will need to be added to our current controls since both VA and DoD users will be working in the same system with both VA and DoD patients. There will be certain population types that will require specialized permissions such as employee health, Vet Centers, non-veteran patients, etc. VA intends to increase our interaction with the private sector over time along with our need

to share information, with and from, the external care community. In addition, our veteran expectations related to self-service continue to grow and will require us to provide more and more self service capabilities that in turn require additional access controls to protect the health care data.

The VA is in the process of investigating alternative methods of issuing our current two factor authentication credentials. While this potential change by VA may alter some of our access processes for issuance, it should not have a significant impact to the use of the two factor credentials by a consuming services such as the EHR. Additionally the VA is implementing an enterprise automated provisioning service. This provisioning service is currently in production and supporting multiple applications, but is not yet deployed enterprise wide. The VA will require the joint VA/DoD EHR to participate in this effort, likely not at initial implementation, but during the span of this contract.

The Contractor shall incorporate VA Identity and Access Management requirements into EHRM system processing. Identity includes support for patient, provider and user identity management. Access Management includes support for multiple authentication methodologies, multiple authentication credentials, digital signature, and supports both high level and granular authorization methodologies based on roles, rules and/or attributes.

The Contractor shall collaborate with VA to determine the number of roles (called positions in the Cerner tools) necessary to perform VA workflows and the association of specific application permissions tied to the roles/positions. The Contractor shall create and maintain all roles/positions within the Cerner provided systems/applications. The Contractor shall provide the technology and interfaces necessary to support both manual and automated provisioning. The Contractor shall support the initial population of users and user permissions during site migration, support long term maintenance of the users and permissions, support VA resources populating and/or maintaining users and permissions, or any combination thereof based upon VA needs. The Contractor shall also provide associated training materials and/or training via a variety of modalities, potentially including in person, to support VA understanding of the new provisioning processes, tools used for provisioning, the available roles and their association to their end users.”

The Contractor shall provide the ability to host VA system components within the same locations as the primary EHR to improve the user experience, response times or to support contingency and continuity situations related to identity and access management (i.e. Online Certificate Service Protocol (OCSP) responders, etc.). It is anticipated this need will fluctuate during the span of this contract based upon system performance, network performance as well as other factors both inside and outside of the Contractor’s control. These needs will be jointly determined by both the government and the Contractor.

5.5.3 **EHRM and VA System Integration**

The Contractor shall identify common VistA interfaces required for all EHRM deployment sites with input from VA. This shall include currently deployed interfaces identified in Section D, Attachment 004 as well as those which VA develops or procures during the performance of this contract. The Contractor shall support all development, documentation including interface control documents, compliance reviews and test activities required by VA to integrate these internal and external systems as required. Integration activities may include, but are not limited to:

a) Existing VistA integrations to external or internal support systems
b) Community Care Clinics – including medical documentation required for provider payment if provided in electronic format.
c) Medical Devices – Internal and External
d) Mobile Apps / Mobile Devices – Internal and External
e) CMOPs

The Contractor shall modify VA legacy systems as required to support integration with EHRM provided that VA will collaborate with the Contractor to share knowledge of the VA legacy systems to support the integration with EHRM. In addition, the Contractor shall provide technical expertise to VA and its Contractors to support integration with EHRM of Commercial software as required. Note that site-specific system interface and legacy system modification may be required as site requirements are identified during deployment. VA will provide access to VA's enterprise InterSystems HealthShare licenses for development of EHRM/VistA interfaces.

The Contractor shall provide interface testing. Tests include steps for nominal and off-nominal interface conditions, minimum and maximum data content, and error handling as outlined in the respective ICD. Data will be verified on each end of the interface to confirm that the correct data is transmitted from EHRM and the data received by EHRM is stored and displayed correctly. Data verification will be automated wherever possible. Finally, [the Contractor shall] provide VA the ability to audit all interface traffic that occurs during testing.

For any new code or code modifications to VA systems by the Contractor, the Contractor shall provide the software build/package including source code and required documentation for release within VA and use the VA approved tool/software code repository which is the Rational tool suite. The Contractor shall change to the new VA code repository if VA transitions from Rational to an internal VA GitHub repository.

For such modifications to VA legacy systems, the Contractor shall create, maintain, and provide the architecture/system diagrams with input from VA for the EHRM and VA systems integration using the DOD Architecture Framework (DoDAF).

To the extent applicable, provide non-commercial and Open Source Software (OSS) source code to support the configuration, integration, custom development, test, software management, training, deployment, and end-user usage of custom developed components of EHRM.

5.5.4 **Data Exchange - Application Program Interface (API) Gateway**

To accelerate better and more responsive service to the Veteran, VA is making a deliberate shift towards becoming a standards-based API driven digital enterprise. A cornerstone of this effort is the setup of a strategic Open API Program, the Digital Veteran Platform API Gateway, that is adopting an outside-in, value-to-business driven approach to create API's that are managed as products to be consumed by developers within and outside of VA.

To support VA's strategic plan, the Contractor shall ensure that all significant data stored in the software is accessible through API's, in other words there will be no need for VA to directly touch the database or data-models and no requirement to create custom applications to specifically access its data. In order do so, the Contractor shall:

a) Deliver and maintain fully tested contractor API Endpoints that return data defined by Cerner or by the latest Cerner supported open standards such as FHIR, Web access to DICOM object (WADO), Integrating the Healthcare Enterprise (IHE), and other Government designated standards.

b) Work with the VA API Gateway team by educating, collaborating, and designing usage patterns of each Cerner API.

c) Establish, operate, monitor, iterate and optimize the infrastructure that will respond to the requests from the VA API Gateway

d) Ensure that the API's, where appropriate, respond with real-time (or near real-time) data through existing architecture or modifications to its architecture.

e) Provide and maintain a Developer Portal(s) that documents each API that is published and provide policies and procedures for the use of the Developer Portal(s) and APIs that promote innovative third-party API development. The portal shall provide a standard, language-agnostic description of APIs which allows both humans and computers to discover and understand the capabilities of the service without access to source code, documentation, or through network traffic inspection. Third party API developers shall retain their IP rights when their API is used to connect to the Cerner interface, and there will be no derivative Contractor IP ownership when third parties consume Cerner terminology through open APIs.

f) As it relates to FHIR, the Contractor shall provide an opportunity for joint collaboration in prioritization of the API roadmap. This support shall occur where VA data required maps to a FHIR (HL7 Fast Healthcare Interoperability

Resources) resource that is currently in the FHIR Roadmap and not part of the software's out-of-the-box FHIR resource offerings

g) Provide a timeframe with VA defining when each endpoint will be absorbed into the core product and will be part of the standard Product Lifecycle Management that benefits from routine upgrades of the product.

h) Ensure that the accesses to data through FHIR API's shall be included in the subscription licenses and there shall be no additional charges for VA to access its own data.

i) Ensure Substitutable Medical Applications and Reusable Technologies (SMART) compliance to support SMART on FHIR applications.

j) The system shall support receiving and processing of approved OAuth tokens to ensure proper user/resource authorized access to the FHIR resources.

k) Provide standards-based API access (e.g. FHIR) to all patient data from the VA-designated authoritative data sources for the patient's record within the Contractors' product suite.

l) Assist the VA in defining and establishing the authoritative data sources associated with each data element in the EHR (e.g., where it is available and who has access to the information, how to further segment or restrict the data, how the data is updated, and any associated core or position "configuration" impacts).

m) Provide the ability for bulk data export and the extraction of bulk data, to include the Common Clinical data set.

5.5.5 **Inventory Management**

The Contractor shall support current VA inventory management systems and methodologies during initial deployments until DoD and VA inventory management methodologies align. The Contractor shall support the aligned inventory management systems and methodologies when implemented.

5.5.6 **Training Plans and Materials**

The Contractor shall create EHRM training management plans and materials for VA review and concurrence. The Contractor shall:

a) Develop and deliver an overall training plan tailored to the VA healthcare environment and workflows covering all EHRM functionality
b) Develop and deliver comprehensive Training Materials tailored to the VA healthcare environment
c) Develop course curriculum and training materials by role aligned to the localized business process and future state workflows of the care team, including relevant SOPs and KPIs by role and task in collaboration with the VA.

d) Plan a training course curriculum per role which will include input from VA Training subject matter experts.
e) Provide training workflows which support the following methods of training at a minimum:
    i. Instructor-led Training (Classroom)
    ii. Digital Media (Computer Based Training, VA hosted Tip Sheets, etc.)
    iii. Over-the-shoulder Training
f) Support remote document collaboration to facilitate knowledge management and change management via Sharepoint. The Contractor shall:
    iv. Provide VA access to Cerner's knowledge management systems as required
    v. Provide VA with documents or links to enable VA to effectively manage EHRM knowledge to meet internal VA requirements
g) Provide VA access to the VTE for training of clinical users as well as local IT, BioMed and other non-clinical system users.
h) Support continuing education and new employee training including topics such as EHR, analytics and HealtheIntent
i) Provide EHRM training materials to the VA Education Group to be loaded in the VA–approved training system
~~j)~~ Provide access to off-site training facilities where space is limited at VA deployment site.

5.5.7 **Organizational Change Management**

The Contractor shall provide national and localized organizational change management strategy, planning and resourcing, with execution of activities to support the adoption of new workflows and the EHRM. The activities will be executed by teams at every level: national, VISN, and facility level (VAMC, CBOC, etc.). The change management teams will consist of appropriately trained and credentialed clinicians, change management specialists, project managers, and operations staff who will support each level according to the needs that are identified through the pre-engagement assessments. Additional teams of these individuals will be available to provide focused support in addition to the Core Change Management Unit. These teams will work with national to establish vision and standards, the VISNs to ensure regional preparation for deployment, and the individual facilities whose staff will be assisted through the deployment phase using the industry-leading change management tactics. The Contractor shall:

a) Facilitate an Executive Alignment Event at the national level that will define or confirm the vision and guiding principles of the project, the project governance, and the value planning, and align leadership to support and lead change throughout the project.

b) Guide identification of Executive Sponsors and Stakeholders, and provide them with the information needed to promote the change with their actions and conversations to increase awareness and desire.

c) Conduct multiple site assessments to determine readiness to change and barriers to adoption at large, integrated, medium, and small facilities as well as CBOCs and other federal facilities as agreed upon with VA
d) Identify change management “hot spots” to align right-sized contract support teams and launch an effective change strategy that plans for process, job, accountability and structure modification.
e) Leverage the the change management methodology agreed by Contractor and VA to document Cerner and non-Cerner options for enterprise variability, then support change management required to standardize processes by facility.
f) Deploy design decision tools at each site to capture and track configuration options, workflows and processes and score the decisions as high, med, low human impact and integrate with deployment teams to support changes.
g) For all change management services contracted by the VA outside of this contract, VA and Contractor will mutually agree on the services provided and mutually set strategic guidance for all change management activities for EHRM as agreed upon by Contractor and VA.
h) Assess change impact readiness to support PMO and facility-specific implementation planning, including potential adoption risks to be mitigated.
i) Determine stakeholder profiles based on role and anticipated impact of implementation and develop communication plans for each stakeholder group.
j) Outline desired cultural attitudes and behaviors and assess the gap from current culture to desired future culture. Create a plan for action to mitigate identified potential barriers.
k) Optimize workflows for each clinical role and functional area and identify impacted clinical and ancillary workflows with functional owners.
l) Support VAMCs in identifying SOPs impacted by Cerner Millennium and HealtheIntent implementation, provide guidance, and facilitate documentation of SOPs to reflect optimized workflows.
m) Define metrics to measure successful change management at the national level, and gain alignment with local stakeholders on relevant metrics. Track and report metrics to leadership, and mitigate ongoing issues and risks as they arise.
n) Identify pain points that may hinder adoption and implement a mitigation plan.
o) Work with Continuous Performance Improvement (CPI) and PMO to identify lessons learned, and contribute to identification of opportunities for improvement of the solution and deployment process.
p) Develop tailored communication plan that spans all stakeholder levels, and develop standard communication artifacts.
q) Identify the necessary skills and behaviors needed to support the change and document requirements for the development of training programs/plans.
r) Establish change networks including change agents at each facility to enable cascading and two-way communication with all impacted staff over the lifecycle of the engagement.
s) Support coordination of parallel charting and mock go-live events using design decision tools to support process standardization.

t) Support site-level training processes with detailed knowledge around specific site related human dynamics and barriers to help improve the individual learning process.
u) Contractor shall provide support to address challenges in organizational structure and alignment identified in the readiness assessment.
v) Provide and execute a change management training strategy to create VA change management super users and facilitate transfer of change management activities to VA support staff.
w) Provide and maintain current-state documentation for use by VA support staff
x) Coordinate hand-off of change management activities to VA support staff in order to maintain the required level of change management support throughout the deployment timeframe.

The Contractor shall facilitate identifying established tasks within workflows and map process and clinical outcomes metrics at the task level. VA will select limited task level metrics to be National Key Performance Indicators. Contractor will facilitate mapping future, enterprise and localized, tasks and workflows to ensure continuity in reporting of task-level metrics and the selected National Key Performance Indicators. The VA and the Contractor will establish method to track progress of this process at each deployment.

For purposes of this PWS, sponsors are supportive of the change and has the influence to gain early buy-in. Sponsors promote the change with their actions, behaviors and conversations. Sponsors can be from anywhere in the organization, but are normally high-level leadership.

Stakeholders are managers, supervisors, and employees who are impacted by the change, but may not have direct oversight or influence over the project. If properly coached these stakeholders are the preferred sender of change messages related to how a change impacts all employees personally. They are essential to convey the WIIFM or 'what's in it for me' message to employees.

5.5.8 **Test and Evaluation**

The VA EHRM Test and Evaluation approach is early engagement of the user community, the VA EHRM test and evaluation community, and the Contractor.

The Contractor shall propose and approach to EHRM test and evaluation strategy including the areas listed below. The VA-approved strategy shall be executed across the VA EHRM deployment timeline with activities starting during EHRM Baseline Preparation and continuing throughout Wave planning and site deployment. The Contractor shall include test & evaluation strategy components including, but not limited to the following:

a) Contractor new development testing activities, joint VA and Contractor data migration testing (covers the data extract, transformation, loading, and data integrity validation) into the EHRM,
b) Contractor testing for functional and non-functional requirements found in the Government RTM including but not limited to interface testing for system integration and interfacing for requirements described in section 5.5.3 EHRM and VA System Integration. Interface testing includes interface connections, message formats, data integrity, data mapping.
c) VA Test and Evaluation activities executed by VA, which can include risk based requirements validation and risk based workflow testing, test observation & validation, system integration/interface & interoperability testing, do no harm testing for VA systems interfaced to the EHRM. VA Test and Evaluation activities for enterprise level requirements, workflows, interfaces are to be completed before the functionality is used before any live site.
d) Site testing such as Integration Validation and medical device testing activities during site deployments

The Contractor shall:

a) Participate in a Test Integration Workgroup that is comprised of VA organizations that have roles and responsibilities in the VA EHRM Test and Evaluation

b) Provide new development testing processes documentation which includes but is not limited to, areas of test design, test traceability, test execution (white box testing, black box testing, regression testing as applicable), and the tools used. For new development that is part of the Generally Available (GA) set of software solutions, the VA may request the ability to verify projects to ensure that they are consistent with ISO and FDA certifications.

c) Provide input and participation into the creation of the VA EHRM Program Test and Evaluation Plan which is developed by the government. The VA EHRM Program Test and Evaluation Plan will describe the overall testing approach and strategy including types of tests planned, define test and evaluation terminology in order to have a common understanding of terminology between the government and contractor, include test activities to be performed and who will perform the test activities, the defect/issue management process during test & evaluation and defect severity definitions that are agreed upon.

d) Create and maintain a Contractor Master Test Plan with input and concurrence from VA EHRM Program Office.

e) Ensure the Contractor Master Test Plan addresses the EHRM's ability to meet the non-functional requirements in the Government RTM particularly performance, scalability, back out of an exception package/patch or rollback to previous version. For non-functional requirements such as performance and scalability, the plan may include such activities as government test observation of

performance testing in Contractor test lab, government analysis of previous performance/abilities testing results, qualifications by similarities evaluation.

f) Provide support for the VA Test and Evaluation including items such as participation in test and evaluations defect/issues process, assistance in troubleshooting/triaging, jointly troubleshooting issues that appear to be development/test environment related, responding to findings from test & evaluation activities.

g) Develop a Test Data Management Plan with input and concurrence by the VA. Interface testing as well as VA Test and Evaluation testing will require the creation and provisioning of test data using enterprise and facility data collection workbooks early enough in either EHRM Baseline preparation or wave planning, site assessment cycle to support interface development, interface testing, and VA Test and Evaluation test events. Test Data within the non-production environments is not allowed to be production data.

   Provide support to VA Test and Evaluation resources in the creation and provision of test data for test events executed by VA Test & Evaluation. Test data creation and provision within the EHRM system for Contractor test events will be provided by the Contractor.

h) Provide user/superuser training and other training identified as required for the VA Test and Evaluation government and contract resources (which can including subject matter experts/members of the user community) to successfully execute test and evaluation activities as early as possible in the EHRM baseline preparation and wave planning deployment timelines. To the maximum extent possible, Contractor shall leverage MHS Genesis training materials that are applicable in areas such as EHRM system functionality common to VA and DoD to provide training as early as possible.

i) Provide an overview and demo of the Contractor's Domains/Environments and Configuration Tools to the Test and Evaluation resources. Presentation will describe the tools, processes and procedures used to configure and interface/integrate to the EHRM. Any overview materials will be provided to VA.

5.5.8.1 **Software Code Quality Checking / Software Assurance**

The Contractor shall have Software Code Quality Checking processes that are executed throughout the development, testing, sustainment of EHRM in accordance with Section D, Attachment 007: SCQC procedures. The Contractor will provide for each VA only EHRM and new development the scanning results reports for each SCQC tools used such as HPE Fortify, WebInspect, Sonar Cube, Findbugs, Dependency Check (OWASP), CAST, or tools of equivalent functionality used by the Contractor within their SCQC program. Remediation Plans documenting the remediation plan of action for critical and high-severity findings will be provided. Scanning reports & Remediation Plan of Actions will be marked as containing sensitive material and will be

delivered with appropriate encryption/secure methods to the VA as results reports and remediation reports are considered sensitive materials. VA EHRM Program office is establishing reciprocity with the DoD MHS GENESIS SCQC program for EHRM modules contained within the MHS Genesis solution.

This requirement applies to EHRM system computer software, including both source code and executable code as determined by joint governance (at least 90 days prior to IOC go-live (for internet facing URLs only) and full package baseline scan minimum once per year), and incremental scans with each patch or full release, specified as a deliverable under this contract.

5.6 **Wave Planning And Deployment**

Wave Planning and Deployment includes all tasks required from initial site assessment through configuration, testing, training, change management, deployment and transition to sustainment.

5.6.1 **Executive Brief**

The Contractor shall conduct an executive brief at each site to communicate deployment goals, outcomes, implementation strategy and to introduce the project team:

a) Review program methodology, governance and facility leadership expectations
b) Begin value objectives for the project
c) Identify site, government and partnership support

5.6.2 **VA Current State Review**

The Contractor shall assess the current state of the site including:

a) Assess current state to gain understanding of current-state operations
b) Ensure personnel are aware of existing service lines and locations
c) Identify site-specific risks or unique areas where updated standards are required.
d) Fine-tune the EHRM user adoption strategy
e) Categorize the level of clinical process change required
f) Provide a checklist of equipment and infrastructure modifications required to support successful deployment
g) Define the value objectives
h) Identify stakeholders
i) Establish local governance through the deployment events

5.6.3 **Future State Review/Workflow Adoption**

The Contractor shall conduct a future state review with site personnel by reviewing Cerner workflows, general business processes and some clinical content to demonstrate enterprise functionality.

The Contractor shall:

a) Provide a visual depiction of EHRM design
b) Review the standard workflows that will be utilized.
c) Review key cross department integrated workflows
d) Initiate critical thinking around what clinical workflows will look like in the future
e) Review gaps identified during current-state debrief and mitigation strategies
f) Continue data collection

5.6.4 **Future state validation**

The Contractor shall conduct a future state validation session to provide users with hands-on exposure to the local build. Workflow configurations identified during the future state review will be reaffirmed and put into action at the FSV.

The Contractor shall:

a) Demonstrate department-level workflows in the localized system with client participation
b) Get hands-on practical application of information acquired during clinical adoption
c) Begin selection of integration validation script content
d) Begin developing test scripts, incorporating value objectives where applicable

5.6.5 **Maintenance training**

The Contractor shall train the VA local IT staff and Biomed staff on local configuration, including areas such as device connectivity and printer set up. Training shall include:

a) Methods for VA users to assist with the installation and preparation activities
b) How to work with the sustainment process post-go-live
c) Clinical areas
d) Specific training for scheduling and surgery personnel on creation and maintaining items such as scheduling templates and preference cards.

5.6.6 **Integration validation**

The Contractor shall conduct integration validation session to ensure that data is flowing properly from EHRM to legacy and other integrated systems during patient scenarios. The Contractor shall:

a) Conduct hands-on testing with site users
b) Evaluate integration testing results to determine conversion readiness.
c) Adjust integration functionality as required for acceptance.

5.6.7 **VA Site Kick-Off**

The Contractor shall conduct VA site kick-off activities. The Contractor shall:

a) coordinate an Executive Leadership Session
b) provide a General Information Session
c) Complete the role assignment workshop
d) Conduct a full site kickoff (Full project team beyond executive officer staff)
e) Begin the site-specific data collection

5.6.8 **Value workshop**

The Contractor shall work with site personnel to identify key value focus areas during deployment. The Contractor shall develop value metrics and standards for evaluating the site EHRM deployment.

5.6.9 **Training**

The Contractor shall conduct site-specific user training including hands on computer courses, interactive classroom instruction and system access for independent practice before go-live. The Contractor shall:

a) Offer computer-based training (CBT) courses prior to instructor-led training (ILT). These courses will be assigned to each user based on his or her new role in the system.
b) Provide trainers to host the ILT at the facility or at an off-site location if facility space is not available.
c) Provide super user training to focus on the EHRM and address common mistakes. Super user training will:

i. Provide an understanding of basic system functionality in the context of department and user group workflows
ii. Provide users with the means to continue independent practice

d) Provide a network of adoption resources and just-in-time training resources for on-the-job support during go-live.

The Contractor shall provide training on HealtheIntent functionality to the appropriate end-user community.

5.6.10 **Go live Readiness Assessment (GLRA)**

The Contractor shall conduct a Go Live Readiness Assessment to help ensure facility readiness. The GLRA shall review, identify and mitigate the individual site's risks and issues prior to go live. After identification of the risks, the Contractor will address the issues until resolution.

The Contractor shall:

a) Identify risks and areas of weakness that could prevent go-live
b) Help ensure mitigation plans are in place to address any concerns

Medication Scanning

The Contractor shall support the VA hospital pharmacies prepare for go live and ongoing maintenance by scanning all medications on formulary before conversion.

The Contractor will assist the VA Super Users and medication administration resources, pharmacy subject matter experts and local IT resources to scan medications and verify that they are stacked correctly in the formulary, and check all medications, including those in: Pharmacy shelves, Narcotics vault (this may require pharmacy staff supervision), IV room, Automated dispensing machines, Central supply, any other holding area that can be given to patients, such as radiology and surgery

Lab Quality Control

The Contractor shall assist VA to run individual lab tests through the proper quality control process to help ensure most frequently performed lab test are fully integrated and produce correct normal and abnormal results and indicators

Hardware rollout

The Contractor shall monitor the status of local IT and facility teams' placement, connection and testing of any new hardware or related infrastructure required for the deployment. This hardware will include such items as label printers, signature pads, monitors and electrical drops.

Mock Go-Live

The Contractor shall conduct mock go-live testing. This facility-led event allows super users to simulate patient flow and test new documentation practices using patient scenarios.

The Contractor shall apply formal training to practical use case scenarios and identify areas needing additional training or workflow practice before go-live

User Configuration and Learning lab

The Contractor shall support events supporting user configuration. These sessions shall enable all end users to:

a) log into the system, change their passwords, synchronize with single sign on (SSO)
b) create their patient lists, customize order creation
c) address other personalization options
d) verify their credentials are appropriate
e) utilize the Learning Lab to try out system features

Go Live Readiness Assessment (GLRA)

The Contractor shall conduct a Go Live Readiness Assessment. The Contractor shall analyze the state of the system and level of staff preparedness in order to present a go live decision to VA for review and concurrence.

Following the GLRA, the Contractor shall deliver a system status and a mitigation plan for outstanding GLRA items. The Contractor shall provide an introduction of the sustainment process following go-live to the deployment site for VA review and approval.

5.6.11 **Test and Evaluation - Deployment**

The Contractor shall:

a) Execute Contractor Master Test and Evaluation Plan conducting the tests and evaluations as described in the plan throughout wave planning & deployments.
b) Provide testing artifacts such as test scenarios, test cases, test results as defined in the EHRM Test and Evaluation Plan

c) Provide support services for the VA test & evaluation including items such as participation in test and evaluations defect/issues process, assistance in troubleshooting/triaging, jointly troubleshooting issues that appear to be development/test environment related, responding to findings from test and evaluation activities.
d) Support readiness reviews such as test readiness review as required by VA and shall compile data for VA submission for readiness and respond to request for changes resulting from those reviews as necessary.
e) Support compliance reviews such as Section 508 compliance review as required by VA and shall compile data for VA submission compliance reviews and respond to request for changes resulting from those reviews as necessary.
f) Provide support to VA resources in the creation and provision of test data for test events executed. Test data creation and provision within the EHRM system for contractor test events will be provided by the contractor.

5.6.12 **Pre-deployment Training**

The Contractor shall employ training methodologies specific to the VA environment and workflows that will meet the needs of end-users, as well as, medical facilities' needs based on information obtained during deployment site visits. Training methodologies will include: instructor-led classroom, Computer Based Training (CBT), and over-the-shoulder training.

The Contractor shall be responsible for providing training to the medical facilities' trainers, as well as, end-users (functional, technical, and administrative). Training for clinical champions, super users, and local trainers will begin at least 90 days prior to Go-Live. Instructor-led training (ILT) for end-users will start at least 60 days prior to Go-Live and will end approximately one week prior to Go-Live to ensure optimal knowledge retention. The Contractor shall provide Over-the-Shoulder training to end-users for at least 90 days post Go-Live. "Train-the-trainer" (T3) training will include clinical champions, super users, and local trainers. Site-specific training timeframes will be specified by VA at the TO level.

The Contractor shall:

a) Propose a training schedule for VA review and approval
b) Customize the national training playbook for site-specific requirements.
c) Provide EHRM training to end-users including but not limited to the following personnel: functional, technical, administrative, and help desk staff
d) Ensure EHRM end-users and trainers obtain the skill sets necessary to utilize EHRM and incorporate it into their daily workflows
e) Validate adequacy of training facilities and resources to meet site training requirements (e.g. computers, printers, projectors, connectivity, etc.) and provide alternate training facilities and/or resources as required
f) Update EHRM Training Materials to reflect site-specific workflows in preparation for training support and change management

g) Develop role based training scenarios for training content aligned to the Business Process Workflows
h) Plan, develop and execute multi-platform training strategies including: instructor-led classroom, CBT, and over-the-shoulder training to ensure preparation and facilitate adoption of EHRM functionality
i) Provide an optional certification training program to VA training staff (trainers/education) that will enable the VA to train and certify VA trainers/end users in the EHRM training content provided by the Contractor
j) Provide enhanced training to super users and clinical champions
k) Administer competency tests and conduct User Experience Satisfaction Surveys in accordance with the Training Materials. Report the percentage of users who have passed the competency test and summary of User Experience Satisfaction Surveys in the Monthly Status Report
l) At the request of VA leadership, update the site training schedule to accommodate Government approved changes.

5.6.13 **Post-deployment Support**

The Contractor shall provide Post Go-Live On-Site Support (OSS) activities for 90 days at the IOC site and 30 days at all subsequent VA deployment locations. Post Go-Live support activities include, but are not limited to, providing 24/7 over-the-shoulder support, troubleshooting system issues, and assisting end-users with workflow support by mapping and gapping the new business processes.

The Contractor shall also provide 24x7x365 Post Go-Live support remotely via the Millennium Service Desk (MSD) and Application Management (AMS) to assist with basic resolution, troubleshooting and configuration as it relates to the Contractor solutions being provided.

5.7 **SUSTAINMENT**

5.7.1 Technical Sustainment

The Contractor shall provide maintenance and support for EHRM software, including Contractor-developed system interfaces, and Cerner-provided hardware at all deployed locations. The Contractor shall ensure that software and hardware maintenance requirements are met. Maintenance consists of upgrades, correcting faults, modifications improving performance or other attributes, and adapting to a changing organization and technical environment. Corrective maintenance will accommodate defects as reported by users. Enhancements or improvements to EHRM will be submitted by the Contractor to the EHRM PMO and subsequently the Configuration Control Board (CCB) for approval.

EHRM sustainment includes all manpower, maintenance, and support activities conducted by the Contractor to ensure the operation and performance of EHRM: this includes the sustainment of all non-production environments through the lifecycle of the system. A VA facility enters sustainment no earlier than Go-Live and no later than completion of post-implementation/Go Live training.

The Contractor shall provide all services and material necessary to perform EHRM sustainment. Sustainment must be in place to support all Government testing. Sustainment includes test items for custom developed code (e.g. test scripts, test cases, test data sets, interface emulators) necessary to support the CCB with regression testing. Sustainment must continue after VA facility Go-Live throughout the PoP of this contract.

The Contractor shall:

a) Provide Millennium Clinical Consultants for over-the-shoulder support assistance and training, liaison assistance with MSD and Application Managed Services (AMS), validation of issues or configuration resolutions, and proactively work with EHRM end-users to improve user experience.
b) Provide Millennium Technical Analysts to provide on-site integration for devices connecting to Contractor system including via the Digital Veterans Platform, local support of the CareAware iBus platform, support for third-party apps connecting to the Contractor system, including via the Digital Veterans Platform, and assistance with any network issues related to the Contractor system.
    i. Coordinate with other vendors and VA local biomedical and IT support staff to troubleshoot and correct technical issues.
    ii. Provide ability for third-party apps to remain connected to the Contractor system without indiscriminately terminating the connection to the Contractor's database(s) except as may be required for security performance and maintenance purposes following notification to VA.
c) Provide Consumer Support to Veterans ensuring they can effectively navigate the HealtheLife patient portal and Wellness programs to effectively manage their health using mobile apps and web-based solutions. Veterans shall be able to enable sharing of their health data with their community care providers in accordance with all VA-designated national standards.
d) Ensure that existing functionality of EHRM including Contractor-developed interfaces is not compromised due to enhancements or updates unless specifically approved by the Government
e) Report on all sustainment activities in the Monthly Progress Report
f) Perform quarterly service review of all sustainment activities
g) Permit and approve connecting all VA approved secure apps using standards based APIs through Contractors CODE (Cerner Open Developer Experience) program. When such apps and connections are for use by VA only, or made available by VA in the Cerner App Gallery, such connections will be without additional mandatoryfees or licensing to VA from Contractor. All other commercial apps, on a case-by-case basis, may be subject to fees and other charges based on Cerner's commercial model; such fees and other charges shall

be comparable to the prevailing commercial rate for other EHRs, which have specialized standards and security considerations.

The Contractor shall provide the following transition planning and support for onsite desktop/device support and onsite training/over the shoulder support:

a) Provide and execute a training strategy to create VA super users and facilitate transfer of activities to VA support staff.
b) Provide and maintain current-state documentation for use by VA support staff.
c) Coordinate hand-off of activities to VA support staff in order to maintain the required level of local support throughout the deployment timeframe.

The level of on-site support required will be determined at the TO level.

5.7.1.1 **Operations and Maintenance**

The Contractor shall provide Application Management Services (AMS) for the Contractor solutions and interfaces which include issue management, troubleshooting, application configuration/maintenance, and proactive monitoring.

The Contractor shall perform the following under AMS:

a) AMS Liaison. Provide a local Engagement Leader (EL) for each VISN and a Regional Client Executive (RCE) for each region to manage the AMS support relationship.
b) Incident Management. Identify, assess impact, report, track, escalate, notify and resolve Incidents that occur within the EHRM applications.
c) Configuration Management. Update or change to ensure effective use of the EHRM applications. This involves building, testing, risk assessment and validation in a non-production environment prior to being configured into the live EHRM system.
d) Change Control. Ensure that the standardized methods and procedures are used and followed for efficient and prompt handling of all changes to the EHRM applications.
e) Content Management. Ensuring that standard content such as Multum, ICD-10, CPT-4 is updated on a monthly, quarterly or yearly basis.
f) Report Management. Maintenance and build of new custom reports (CCL, PowerInisght, Discern, etc.) needed for the EHRM applications.
g) 24x7x365 Application Monitoring. The process that measures and evaluates the performance of an application and provides the means to isolate and rectify any abnormalities or failures. Transactions being monitored include:
    i. Operations Jobs
    ii. Print Jobs
    iii. Chart Servers
    iv. Faxing
    v. Interfaces
    vi. iBus Connectivity

h) Proactive Reviews. Provide reviews and recommendations of Light's On application performance and application audits to ensure optimal EHRM application performance.
i) Problem Management. Identify root cause and corrective or preventative action for one or more Incidents.
j) Monthly Reporting. Provide reporting on service performance metrics, proactive reviews, progress updates on outstanding issues, and identification of continues improvement opportunities.
k) Provide and execute an operations and maintenance regional alignment training strategy to create VA regional alignment super users and facilitate transfer of regional alignment activities to VA support staff.
l) Provide and maintain current-state documentation for use by VA support staff.
m) Coordinate hand-off of regional alignment activities to VA support staff in order to maintain the required level of regional alignment support throughout the deployment timeframe.

5.7.1.2 **Help Desk Support**

The Contractor shall provide functional and technical support for EHRM System incidents. The Contractor shall be capable of providing two separate levels of support as VA transitions to a new internal service desk solution. These levels of support are defined as:

a) Gold level support of all EHRM troubleshooting where all trouble calls are received by the Contractor's Millennium Service Desk (MSD) for resolution. The Contractor shall provide additional support as required through Cerner local onsite IT support and remote Application Management Services (AMS). Trouble tickets not resolved by MSD will be escalated to AMS.
b) Silver level support where EHRM service desk calls will be received by the VA ESD who will create a ticket in the VA IT Service Management tool. ESD will determine if the ticket can be resolved within ESD, or should be escalated to local IT, other VA support, or routed to the Contractor MSD. The Contractor shall provide ESD support staff with Knowledge Base documentation and appropriate training to ESD SMEs for VA ESD Tier 1 support of the EHRM application. The Contractor shall support initial on-site support to the VA ESD service providers to facilitate transition to EHRM. Trouble tickets not resolved by MSD will be escalated to AMS.

The Contractor shall receive, analyze, and resolve all assigned trouble tickets. VA will be responsible for password resets as well as incidents related to non-Contractor systems. Account provisioning will be a combination VA / Cerner responsibility. VA will maintain the identification of role provisioning. The Contractor shall perform the system work within the system boundary, whether manual or automated, to provision VA authorized users.

The Contractor shall provide MSD support including but not limited to:

a) 24x7x365 coverage (after hours, weekends and holidays)
b) Quick resolution of issues through incident and problem management
c) Provide consistent, personable, helpful communication
d) Contractor solution knowledge upon first contact
e) Provide transactional client satisfactions surveys
f) Call recording
g) Shadowing to increase speed to resolution
h) On-site support at each deployment site throughout the PoP
i) Monthly statistical reporting
j) Information gathering for deeper troubleshooting by AMS

The Contractor shall:

a) Coordinate Cerner and VA service desk processes and language, including ticket grouping, severity assignment, categorization and ticket classification
    a. Accept warm hand-off calls from VA ESD
b) Provide support to the VA ESD Help Desk in EHRM ticketing resolution and communication where appropriate.
    I. Communicate all EHRM System updates, including hardware and software, to the VA ESD Help Desk
    II. Make SMEs available to support staff
    III. Provide technical troubleshooting and fixes for trouble tickets
c) Provide bi-directional interface to the Enterprise Service Desk (ESD) COTS ticketing system via established APIs ensuring that relevant resolution information is updated to the ESD ticket. Note: Tickets closed by Cerner can be marked as closed in Cerner's ticketing tool. Only VA can mark a VA ESD ticket as closed in VA's ticketing tool.
d) Receive, log, and track incident and trouble tickets from VA ESD for entry to the MSD process
e) VA ESD reserves the right to implement a different trouble ticket management tool at any time
f) Any ticket issued with patient safety implications will be fast tracked, resolved as quickly as possible and reported back to the VA ESD
g) Pass any incidents received by MSD that do not relate to the Contractor system back to the VA ESD Help Desk for troubleshooting and resolution
h) Respond to incident tickets within standard criticality response times
i) Provide number and trends in tickets in the Monthly Progress Report

In addition, the Contractor shall provide 24/7/365 Consumer Support to Veterans to resolve technical issues with the HealtheLife patient portal and Wellness programs including access, navigation and third-party device integration concerns.

The Contractor shall provide the following transition planning and support for Millennium Services Help Desk, Millennium Services Help Desk – Provisioning, and Consumer Help Desk (Wellness and Portal):

a) Provide and execute a training strategy to create VA super users and facilitate transfer of activities to VA support staff.
b) Provide and maintain current-state documentation for use by VA support staff.
c) Coordinate hand-off of activities to VA support staff in order to maintain the required level of support throughout the deployment timeframe.

If trouble ticket resolution fails to meet the 'Application Incident Resolution' times set forth below, then the VA Contracting Officer reserves the right to initiate contract remediation actions as appropriate. Specifically, the Government may issue a unilateral stop work order at no cost to the Government, however, the Contractor will not stop work on resolving to the Government's satisfaction, performance issues related to the 'Application Incident Resolution' time. Notwithstanding the foregoing, the Government may utilize any contract remedies, inclusive of but not limited to, cure notice, show cause, notice of termination, and/or financial penalty as set forth in the contract.

Priority	Resolution Time SLA	Frequency
Application Incident Resolution		
Critical	100% of trouble tickets resolved* or mitigated through VA approved mitigation strategy, within 5 hours Completely resolved** within 24 hours	Continuous
High	90% of trouble tickets resolved within 16 hours AND no single ticket exceeds 64 hours	Monthly
Moderate	80% of trouble tickets resolved within 4 business days AND no single ticket exceeds 60 calendar days	Monthly
Minor	80% of trouble tickets resolved within 6 business days AND no single ticket exceeds 60 calendar days	Monthly

*A ticket is considered 'resolved' when Cerner places the ticket in a 'Client Action' status for the client to approve / confirm the issue is addressed.
** A ticket is considered 'completely resolved' when VA has had approved and confirmed that a trouble ticket placed in "Client Action" has been fully addressed. Once VA confirms that the ticket has been completely resolved, Cerner is responsible to close the ticket..

VA may provide an oversight and audit role to ensure tickets are correctly assigned to the right priority.

Incident Code Descriptions	
Incident	**Description**
Critical	A patient care or safety condition exists; **OR** Major percent (greater than 25%) of concurrent users across a VAMC and associated facilities are unable to process transactions or access managed solutions critical to their ability to conduct daily business **AND** No bypass or alternative is available **AND/OR** Major financial impact* to VA
High	Significant percentage (15-25%) of concurrent users across a VAMC and associated facilities are unable to process transactions or access managed solutions required to conduct daily business **OR** A component of Managed Software required to complete a critical workflow is non-functional for more than one (1) user **AND**

	No bypass or alternative is available **AND/OR** Financial impact** to VA
Moderate	A component, minor solution, or procedure is down, unusable, or difficult to use. There is some operational impact but no immediate impact on service delivery, financial, or patient care. An acceptable workaround, alternative or bypass exists. One or more Client locations are impacted. Problems that would be considered critical or high that have an acceptable workaround, alternative, or bypass available will be assigned as a moderate Incident.
Minor	A component, procedure or personal application (not critical to Client) is unusable. No impact to business, single Incident failure, and an acceptable workaround, alternative, or bypass is available. Deferred maintenance is acceptable.
Resolution Time	The Application Incident Response SLA performance time for a resolution will be calculated as the difference between the time a request is "opened" in Cerner tracking tool and the time the request is documented as "closed" in Cerner tracking tool, less the time the Incident is in "Client Action" in Cerner tracking tool. An Incident is considered in "Client Action" when Cerner is asking Client a question or when Cerner is requesting information from Client or for the duration of Client validation. The Application Incident Response SLA performance time for requests needing a software change (software defect or software enhancement) will be calculated from the time the request is "opened" in Cerner tracking tool until the time the request is identified as needing a software change, less the time the request is in "Client Action" in Cerner tracking tool. The request will be closed in the Cerner tracking tool at the time the software change is identified and will be tracked via Cerner software release process.

*Affecting the VA overall organization, i.e. all sites would be affected by the issue.
**A single organization is affected.

5.7.1.3 **Sustainment Testing**

Sustainment testing are activities for upgrades to the EHRM system. All upgrades, exception packages/patches will go through the change control board processes.

The Contractor through the Contractors Upgrade Center Managed Services (UCMS) shall:

a) Provide the non-production environment (mock domain), test data, for contractor and VA Test & Evaluation sustainment testing, and installation.

b) Provide test cases, scripts and perform contractor regression testing, continuous package testing.

c) Provide support services for EHRM VA Test & Evaluation sustainment testing which may include VA interface regression testing; user EHRM system and integration validation testing. Support services include responding to issues found during VA sustainment testing, resolving issues/fixing and documenting

fixes, and repeating sustainment testing cycle as necessary. Exit criteria will be defined for VA sustainment testing and the move to production installation.

d) Install upgrade into production after exit criteria for sustainment testing and appropriate CCB approvals are completed.

5.7.1.4 **Technical Sustainment Training**

The Contractor shall:

a) Provide ongoing sustainment support, including but not limited to, training EHRM System users and IT support staff, maintaining training materials, supporting business process reengineering and change management efforts
    i. Provide an Implementation Plan to propose a regional sustainment team structure
b) Provide training to training staff which includes:
    i. Certification Training
    ii. Training for software patches, updates, and new releases
c) Optimization Training
d) Deliver updated EHRM System Training Materials
e) Maintain and update the Virtual Training Environment to reflect any updates to the production environment
f) Provide additional training as required by the Government, such as, but not limited, to surge training and mobile training

5.7.1.5 Upgrade Services

The Contractor shall:

a) Plan, build, test, and deploy EHRM System releases
b) Identify and manage risks to successfully deploy each EHRM System release
c) Establish a common understanding of each EHRM System release between the Functional, Business and Technical Stakeholders
d) Coordinate release with the system development lifecycle components: Engineering Management, Program/Project Management, Requirements Management, Development Management, Cybersecurity Management, Infrastructure Management, Logistics & Lifecycle Sustainment Management, Test Execution, Change and Configuration Management, Transition Planning, Scheduling, and Build and Deployment Management

5.7.2 **End-User Sustainment**

5.7.2.1 **End-User Sustainment Training**

The Contractor shall provide EHRM specific training courses for new hire/new resident programs. The courses will apply to EHRM impacted end-users (functional, technical, and administrative) beginning 30 days post go-live for VA deployment locations with the exception of the IOC site which would start 90 days post go-live, per the post-deployment support plan.

The Contractor shall:

a. Work with the TO level to propose a new hire/new resident EHRM impacted role training schedule for VA review and approval
b. Plan, develop and execute multi-platform training strategies including: instructor-led classroom, CBT, and over-the-shoulder training to ensure preparation and facilitate adoption of EHRM functionality for new hire/new residents
c. Develop role based training scenarios for training content aligned to the Business Process Workflows for incorporation in new hire/new resident EHRM training
d. Provide EHRM training opportunities to new hire end-users/new residents including the following personnel: functional, technical, administrative, and help desk staff
e. Ensure new hire EHRM end-users obtain the foundational skill sets necessary to utilize EHRM and incorporate it into their daily duties
f. Validate adequacy of training facilities and resources to meet site training requirements (e.g. computers, printers, projectors, connectivity, etc.) and provide alternate training facilities and/or resources as required
g. Annually update EHRM post-deployment training materials to reflect lessons learned to ensure EHRM new hire/new residents are benefiting from past experiences
h. Provide an optional certification training program to VA training staff (trainers/education) that will enable the VA to train and certify VA trainers/end users in the new hire EHRM training content provided by the Contractor

5.7.2.2 **Workflow Analysis and Optimization**

The Contractor shall:

a) Continuously assess industry best practices and recommend improvements for the most efficient and effective business workflows for EHRM
b) Participate in Business Process Reengineering (BPR) Integrated Product Teams (IPTs)
c) Conduct ongoing analyses of current EHRM System workflows to provide recommendations on process re-engineering, change management, and product configuration
d) Utilize EHRM data to assess clinician use of system functions and technical statistics on system performance
e) Take proactive steps to determine and implement improvements to user processes and the effectiveness of services delivered

5.8 BUSINESS INTELLIGENCE,DATA ANALYTICS, AND POINT OF CARE DECISION SUPPORT

The Contractor shall support business intelligence and data analytics including such items as:

a) Defining, through VA and Contractor governance, the applicable VA reports to migrate to Cerner technology and environments
b) Extraction and analysis of EHRM data by facility, Veterans Integrated Service Network (VISN), Region and enterprise levels
c) Include data from Cerner sites in key VA reports and in databases used for important performance and quality improvement initiatives.
d) Provisioning of robust data analysis toolsets that allow for web reporting, trending, forecasting, machine learning, and large scale multivariate analysis to include VA-generated reports, registries, health services research, analytics and Clinical Decision Support (CDS), exploratory analytics and near-real-time CDS, and syndication to VA and VA partners such as Oak Ridge National Lab (and potentially other directed environments) for exploratory analytics and near-real-time CDS.
e) Develop a plan through joint governance to evaluate feasibility and methods of including VA tools and technologies (i.e. reporting tools and capabilities) to access and analyze data within Contractor platforms.
f) Provide the ability to index and search on key words and terminology contained in VA clinical notes and return or link to those documents that contain the words or phrases of interest.
g) Provide the ability to provision and maintain data marts around specific clinical or administrative subject areas and utilize provided reporting and analytic tools to report and analyze the data
h) Provide the VA EHRM data model, underpinning terminology model, tables, definitions, and examples of fully populated Veteran data files to the VA. Provide the VA with documentation or software that is used for quality checks and that illustrate what data elements are computable.

The Contractor shall:

a) Leverage VA PMO to facilitate and conduct initial meetings with existing VA reporting, analytics, and business intelligence Programs foremost of which are the VHA CDW and VBA EDW warehouse solutions. During these meetings we will baseline the critical reports that are maintained within these warehouses and will capture information on the frequency, formats, and data sources used to generate the reports. The outcome of these initial meetings will be a high-level inventory and baseline of critical reports that will migrate to Cerner technology solutions. The Contractor shall allow access by VA and any VA-designated parties to all tools/data required for report generation.
b) Bring together the proper governance bodies (e.g., Executive Governance Board, Functional Governance Board) and establish a Reporting Transition Tiger Team. This Team will review and assess the current reporting products,

identify modifications and/or new reporting needs, and develop a prioritized list of report transition (or development) items. The Tiger Team will brief out and obtain approval from the Executive and Functional governance boards on the reporting strategy and initial prioritization scheme. The Tiger Team will brief its activities as an agenda item at recurring governance meetings to revise the reporting strategy and priorities as required.

c) Perform report migration using Cerner technologies to include HealtheIntent and HealthEDW as well as using other commercial reporting tools such as Tableau.

5.9 **Analysis And Migration Of Legacy Data**

The Contractor shall execute the following data migrations in alignment with the EHRM wave deployment schedule. Data migrations include:

a) VA clinical data migrated to HealtheIntent – initially 15 domains
b) Non-DICOM Images
c) DICOM images
    i. Reference
    ii. Diagnostic quality

Additional migrations shall occur following the overall EHRM schedule:

a) Bulk VA data from HealtheIntent to Millenium – initially 5 domains
    i. Initially PAMPI: Problems, Allergies, Medications, Procedures, Immunization
    ii. Moving to PAMPI+
    iii. DICOM imaging and imaged documents and other multi-media will not be included In the initial phases of migration.
b) Iterative migration of remaining VistA clinical, dental, administrative and financial data that is relevant for clinical care, registries, reporting, or analytics to additional domains in HealtheIntent and/or Millenium Priorities will be determined by the Data Governance Board.
c) Migration or archiving of remaining VistA data per direction of the Data Governance Board to enable retirement of VistA instances.

The Contractor shall develop the data processing scripts including terminology mapping to standards and information model transformation.

The Contractor shall migrate VistA legacy data into HealtheIntent utilizing a historical bulk load and an ongoing update stream during the deployment time period based upon the following process:

a) VA will physically transport the historical load to the Cerner Data Center and restore onto an environment established for hosting VA data;
b) VA will manage the ongoing update stream;
c) The Contractor will ingest, aggregate, normalize and standardize the VA data into HealtheIntent and/or Millennium by a predetermined method.

5.10 Innovation and Enhancements

5.10.1 Innovation Process

The Contractor shall work with VA to identify innovations through a VA/Cerner Innovations Governance Board. The Innovations Governance Board will serve as the decision-making body for approving innovation projects, identifying and allocating resources and investments, and resolving issues when they arise. The innovations governance structure shall be consistent with the overall future-requirements governance. Joint Governance will review and prioritize VA's Informatics and Interoperability requirements included in Section D, Attachment 003: Non-Functional RTM.

The Innovations Governance Board will:

a) Be responsible for governing all aspects of the innovation relationship including strategy, priorities, resourcing, and performance oversight. Resourcing will be identified for each phase of the software/data-development lifecycle;
b) Consist of an equal number of senior leaders from VA and the Contractor;

The Contractor shall support the process for managing innovation ideas from conception to execution with technical support including access to the appropriate commercial environment. The staged innovation process includes idea creation, development, launch and commercialization. As part of performance oversight and in conformance with the current governance plan, the Innovations Governance Board will make a go/no go decision to continue at the end of each stage in the process.

5.10.2 Innovation Categories

After an innovation is approved, the innovation will be categorized as one of the following:

a) An evolution of a module of Contractor's commercial off the shelf software. Evolution innovations will typically be made generally available by Contractor and will be provided to VA subject to the terms of the EULA set forth in Section D.
b) A configuration involving the use of Contractor tools to provide a unique capability. For example, Cerner MPages allows for customized views and

workflows in the EHRM, which would be a minor modification of a commercial item

c) A configuration involving the use of Contractor tools to provide a unique capability that is more than a minor modification of a commercial item, and is first produced and delivered under this Contract could be licensed under 52.227-14 (owned by Contractor but provided with unlimited rights to VA) and subsequently made available under an open source license such as APACHE, Version 2.

d) An extension of the EHRM using either Contractor-dependent or independent technology. An example of an extension includes a new application such as a growth chart application or medication adherence application. An independent application may use Fast Healthcare Interoperability Resources (FHIR) and a SMART container to visualize the application in the EHRM. An example of a Contractor-dependent innovation is a similar application that leverages Contractor proprietary objects-oriented technologies and APIs to connect the application to the EHRM. The Task Order will describe the specific requirements of Contractor to sustain the extension. An extension will typically be owned by Contractor and licensed to the VA with unlimited rights and subsequently made available under an open source license such as APACHE, Version 2.

e) An open innovation is a foundational, platform independent technology that may be utilized with Contractor solutions but has independent value outside of Contractor's platforms. Examples include Cerner terminologies, ontologies, methods of developing healthcare IT content, standards processes and rules, for example, such as those employed to program Cerner's population health solutions. Open innovation Intellectual Property (IP) will be committed to an open source community or public domain, as appropriate and mutually agreed to in a Task Order, by Contractor and the VA when such open innovation IP is necessary to realize a standardized implementation of platform-independent healthcare IT content.

f) A joint contribution is an innovation created and developed by Contractor and the VA. If the VA is not contributing funds, then a CRADA may be negotiated to facilitate the Joint Contribution in coordination with the VA Technology Transfer Program (TTP). The VA may receive consideration in the form of software allowances, future licensing discounts, or other remuneration, according to parameters and amounts previously agreed by the Innovations Governance Board as documented in a written agreement subsequently incorporated into this contract or one of its Task orders, and joint inventors of patented inventions may receive royalties in these arrangements in accordance with patent license agreements to be established that are consistent with Contract Clause, Patent Rights – Ownership by the Contractor, FAR 52.227-11, (DEC 2007). If the VA is also contributing funds, then an alternative cooperative development agreement may be required for

Joint Contributions. Joint Innovations made in concert with the DoD may be developed under an Other Transaction Authority (OTA) agreement.

g) A knowledge sharing innovation is a contribution to a standards organization or consortium to advance the knowledge set of the industry at large. Examples include contributions made to the ONC as part of the Direct Project or the CommonWell Health Alliance.

Specific detailed plans for each approved innovation will be defined in a Task Order (or other appropriate vehicle). Each Task Order will include the purpose of the innovation, categorization of the innovation as detailed above, scope of work and schedule of completion. The Task Orders will also identify each party's responsibilities and deliverables as well as intellectual property rights, such as ownership and applicable use license rights.

5.10.3 **Other Development Activities**

For other custom software development, Contractor shall follow its commercial development processes as well as the following activities:

a) Document development requirements in a Task Order;
b) Document any dependencies, if applicable, to reflect implementation and configuration of custom configuration item;
c) Ensure compatibility with applicable hardware and software within the existing processing environment; and
d) Maintain traceability of custom software design to meet the requirements specified in the Government RTM, if applicable.

5.10.4 **Seamless Interoperability / Joint Industry Outreach**

The Contractor is required to collaborate with VA affiliates, community partners, EHR providers, healthcare providers, and vendors to advance seamless care throughout the health care provider market. Seamless care will require the creation of an integrated inpatient and outpatient solution with software components that have been designed, integrated, maintained, and deployed with a design architecture that allows for access to and sharing of common data and an enabling security framework that supports end-to-end healthcare related clinical and business operations. Seamless care is the experience patients and providers have moving from task to task and encounter to encounter within or between organizations such that high-quality decisions form easily and complete care plans execute smoothly. Information systems support the seamless-care experience by gathering data, interpreting data, presenting information, and managing tasks. Currently, industry lacks specific and uniform interoperability standards to support seamless care between organizations that employ different EHR systems. The Requirements Traceability Matrix Section D, Attachment 003, sets forth specific

Informatics and Interoperability contract requirements. To accomplish this, the Contractor shall provide software and services to enable seamless care between VA encounters, encounters with other Government healthcare institutions, and outside entities through advancements in all areas of the EHR that occur. In addition, the software and services shall support the VA designated standards, such as SMART on FHIR and SMART-enabled applications, or other published standards.

The objective of these interoperability solutions is to advance the state of the art supporting seamless care for Veterans. Existing organizations promoting interoperability among EHR vendors, such as The Argonaut Project, have developed or are planning to develop technology standards or technical approaches that may support the EHRM seamless care strategy. To the extent that underlying third party technology is available or made available to meet the following timelines, the following interoperability software solutions and services shall be delivered under this section:

a) By Initial Operating Capability (IOC), the Contractor shall provide a software solution enabling VA, DoD and community providers who have connected to the EHRM to share interactive care plans (ICPs) for Veterans. ICPs will enable collaborative communication between providers, and between providers and Veterans, in managing Veteran care.
b) Within 24 months of applicable task order award, the Contractor shall provide a software solution enabling VA, DoD and connected community providers to complete referral management activities for Veterans.
c) By IOC, the Contractor shall provide a software solution enabling VA to release and consume, via on-demand access, a Veteran's complete longitudinal health record or discrete data elements, as needed, to and from DoD and connected community partners, irrespective of which health IT module or system is being used, provided such health IT module is certified to the most recent version of the ONC's certification program or its successor. The longitudinal record solution shall support Provider-to-Provider record sharing, as well as Provider-Veteran-Provider sharing (Veteran mediated record sharing), including appropriate consent management. The bi-directional health information exchange shall maximize use of discrete data that supports context-driven clinical decisions and informatics.
d) Within 24 months of applicable task order award, the Contractor shall provide a software solution enabling connected VA, DoD and community providers connected to the EHRM to send and receive Admission/Discharge/Transfer-based notifications "pushed" from the provider initiating a Veteran care event to enable proactive engagement by VA care coordinators when notified of a Veteran care event.
e) Within 24 months of applicable task order award, the Contractor will demonstrate a solution for identification and management of Veterans at high risk of suicide, in collaboration with community partners.
f) By IOC, the Contractor shall provide URL based image access to the VA, community and academic partner via URLs embedded in radiology reports associated with a particular episode of care and available for sharing via health information exchanges. Within 36 months of applicable task order award, the

Contractor shall provide a software solution enabling VA, DoD and community providers connected to the EHRM to have nationwide access to Veterans' imaging associated with diagnostic tests.

g) By IOC, the Contractor shall provide a software solution for multilateral standards-based ingestion, normalization, storage, and exporting of acquired Veteran health information. The Contractor shall ensure that the solution provides a computable dataset for purposes of population health and research analytics, clinical decision support, and workflow integration.
h) By IOC, the Contractor shall provide the capability to connect and exchange VA electronic health records via other interoperable networks, specifically, but not limited to, CommonWell Health Alliance and DirectTrust by supporting their specifications, security and content specifications. When available, the Contractor shall participate in a Health Information Network (HIN) or Qualified Health Information Network (QHIN) that has agreed to the terms of the Trusted Exchange Framework and Common Agreement (TEFCA). Participation is defined as being in production with a HIN or QHIN, under a participation agreement that aligns with the TEFCA.
i) By IOC, the Contractor shall provide a capability for provider collaboration via secure e-mail using the ONC Direct protocol or future VA-designated standard within a Cerner Millennium EHR workflow context.
j) Within 36 months of applicable task order award, the Contractor shall provide a solution for a Software Development Kit (SDK) enabling standards-based applications (e.g., SMART, FHIR, WADO etc.) integrated with EHRM solutions and platforms.
k) Cerner shall deliver annually an Interoperability Plan to the VA on how it intends to meet the objectives established in PWS section 5.10.4. The initial plan will be due within 3 months of applicable TO award.
l) The Contractor shall conduct an annual Interoperability Self-Assessment against standards that shall be specified by VA**,** such as those promulgated by HIMSS or future standards to be identified by VA. The annual self assessment shall report on the state of each data element (e.g., which are supported in what capacities and in which formats). This will help assure standards implementation consistency and assure standards compliance with evolving national standards.
m) The Contractor shall support Knowledge Interoperability by supporting the extension of clinical content assets such as terminologies, clinical decision support rules, and order sets, etc., to the extent such extensions are consistent with the model and best practices of the controlling national standard. This includes the ability to curate, extend, and share that knowledge with clinical partners. This fosters rapid adoption from industry best practices, e.g., clinical professional societies.

5.10.4.1 Data Design and Information Sharing

In support of the interoperability objectives under this Section, agreed upon Contractor proprietary information/data model extension points (e.g. ingestion and record APIs)

may be provided to both international and national standards designating organizations as described and set forth in an applicable Task Order. The Contractor shall provide VA access and usage rights into any underlying proprietary terminology/code systems for the purpose of enhancing national standards to address any gaps identified in the EHRM solution. The Contractor shall also make the interoperability capabilities and product enhancements developed under this contract available to non-VA Cerner clients.

5.10.4.2 VA Digital Health Platform/Digital Veterans Platform Integration

VA anticipates developing a Digital Health Platform/Digital Veterans Platform (DVP) to consolidate critical VA EHR and non-EHR operational systems. The Contractor shall integrate the EHRM to interoperate with DVP, or future state VA platform, including the DVP API gateway or any other method designated by VA.

5.11 APPLIED INFORMATICS INSTITUTE

In close collaboration with VA subject matter experts, the Contractor shall create an adult-learner focused institute that provides flexible, multi-disciplinary professional development programs around topics including informatics (e.g. fundamentals, clinical decision making, care process improvement, health information systems, leading and managing change, analytics and data management) and Cerner-specific approaches (e.g. methodology, culture, management, and leadership). The organization will serve two populations and distinct purposes: 1) enhance and transform VA staff professional skillset to support and lead a modern EHR platform and 2) optimally prepare individuals (partners/3rd parties) to support the VA's EHR program.
The Contractor shall build services and a longitudinal support mechanism that promotes individual enrichment and achievement beyond end-user technical (day-to-day system use) knowledge including:

a) Deliver a comprehensive learning eco-system that promotes role-based professional development in settings focused on the delivery of healthcare.
b) Provide curricula, including opportunities for team-based learning activities, for multi-disciplinary VA staff that support a variety of healthcare informatics roles.
c) Provide standardized onboarding curriculum for Partners / 3rd Parties that varies by project role (EL, IA, Consultant, Change Management, etc.).
d) Offer course catalogs (by track and/or role) outlining required and elective courses and experiences.
e) Provide multiple exposure-points, including face to face as well as virtual training, and support through a variety of synchronous/ asynchronous and individual/team-based learning vehicles and that evolve as new functionality, products, and approaches are developed.
f) Deliver high-volume courses, such as end-user and super-user training at local deployment sites.

g) Course delivery will take place predominately in Kansas City (KC) with roughly 20% of the courses taking place in locations (in continental US) outside of KC; locations outside KC will be mutually agreed upon by VA and Contractor. High volume courses (such as super-user training) will be provided locally when possible to minimize travel time. Training spaces will be adequate for the design of the course and appropriately organized to meet the needs of the learners and the design of the course.
h) Ensure and maintain academic quality and rigor in course design and through continuous evaluation and feedback mechanisms. Provide individual feedback to participants and summary reports to advisory board and managers as applicable.
i) Provide recognition of achievement through appropriate designation (certificate, diploma or contact hours).
j) Support interoperability symposiums and health conferences
k) Create a blended Contractor and VA advisory board that provides input on strategic direction and planning.

The Contractor shall provide technical support and strategic input to VA's effort to expand up to two VA SimLearn centers to accommodate a training environment with equivalent functionality to the Applied Informatics Institue.

The Contractor shall provide the following transition planning and support for the Applied Informatics Institute:

a) Provide and execute a training strategy to create VA super users and facilitate transfer of Applied Informatics Institute training activities to VA support staff.
b) Provide and maintain current-state documentation for use by VA training staff.
c) Coordinate hand-off of activities to VA training staff in order to maintain the required level of support throughout the deployment timeframe.

5.12 **EHRM Technical Support**

Throughout the PoP, there may be requirements for EHRM hardware, software development and/or technical input in support of the enterprise solution, to accommodate new VA facilities, clinical practices, new standards or other developments inherent to the EHRM solution. The Government will utilize the proposed firm fixed price labor rates which shall be incorporated into the order at time of award as set forth in the Price Schedule.

This support may include such items as the following:
VA expects that during the life of the contract there will be new and innovative technologies and standards that improve the user experience, enhance security/privacy or improve interaction with the customer or the community. VA may choose to add these new or innovative technologies or standards to the EHR.

5.13 **Transition Support**

The Contractor shall recognize that, in accordance with FAR 52.237-03 the services under this contract are vital to the Government and must be continued without interruption, and that upon contract expiration a successor, either the Government or another contractor may continue them. The Contractor shall provide phase in training and exercise its best efforts and cooperation to effect an orderly and efficient transition to a successor.

The Contractor shall develop a Transition Plan supporting 90 days of outgoing transition support. Upon VA PM's approval of the Transition Plan, the Contractor shall commence transition out activities working with the incoming Contractor or Government entity. Additionally, the Contractor shall provide formal coordination with Government staff and successor staff and management. The Transition Plan shall specify a training program and a date for transferring responsibilities for each division of work described in the plan. The Contractor shall provide sufficient experienced personnel during the phase-in, phase-out period to ensure that the services called for by this contract are maintained at the required level of proficiency. The Transition Plan shall include, but is not limited to:

a) Coordination with Government representatives
b) Review, evaluation and transition of current support services
c) Transition of historic data and EHRM Data in a structured format conforming to current storage and access technologies to VA or to a new Contractor system
d) Transition of all accounts
e) Disposition of Contractor purchased Government owned assets,
f) Transfer of Government Furnished Equipment (GFE) and Government Furnished Information, and GFE inventory management assistance
g) Turn-in of all Government keys, ID/access cards, and security codes

The Contractor shall provide the VA PM and COR a bi-weekly status of the level of effort expended on this task.

5.13.1 **Transition Services for Revenue Cycle**

The Contractor shall provide dedicated revenue cycle specialists to help augment and manage accounts receivable during the transition from the legacy system to Cerner Revenue Cycle solutions. The transition services provided will include:

a) Starting prior to each individual go-live of the revenue cycle solutions, contractor shall provided a fixed number of offsite dedicated medical billing specialist resources. Resources will provided support for a period of twelve (12) months.
b) Contractor will monitor standard reporting metrics produced by the applicable solution(s).
c) Monitor of work queue volumes and client work flows.
d) Work to perform edits and rejections in Patient Accounting solution as well as the claims scrubber.
e) Client is responsible for the management and reporting of all receivables in legacy solutions.

5.14 **Standards and Certifications**

The Contractor shall work closely with VA to advance the goal of seamless interoperability as described above in 5.10.4: Seamless Interoperability / Joint Industry Outreach. Seamless interoperability will require the Contractor and VA to continually evolve to meet the current state of data standards, processes, and certifications as they become active throughout the Period of Performance of this contract. The plans, standards, and certifications identified below are a starting point for EHRM compliance with the current state of data interoperability. The Contractor will support current interoperability standards and specifications identified in this section as required for features and capabilities directed for delivery by VA. Additional and/or updated standards will be added over time as they become active. The Contractor shall make available in production updated standards and certification requirements approved by joint VA/DoD governance within 18 months of those standards and certification requirements becoming active unless earlier implementation is indicated at a task order level.

The Contractor shall maintain certification to the current version of the Certification Criteria published by ONC and listed below. The Contractor shall update and release products in compliance with the updated versions of the Certification Criteria within 18 months of that version becoming active.

Current ONC Certification:

- 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications: Final Rule - October 6, 2015.

The Contractor shall support the generation of FHIR resources in multiple versions, profiles and implementation guides that are compatible in parallel (e.g.: DTSI 1.0, DTSU 2.0; Argonaut, US Core).

Current FHIR Specifications

- *Fast Healthcare Interoperability Resources (FHIR) Draft Standard for Trial Use (DSTU) 2 (v1.0.2-7202)*

Current Implementation Specifications:

- *Argonaut Data Query Implementation Guide Version 1.0.0*
- *Argonaut Data Query Implementation Guide Server*
- *SMART App Authorization Guide:* http://docs.smarthealthit.org/authorization/
- *OpenID Connect Core 1.0 incorporating errata set 1*
- *Consent2Share (C2S) FHIR Consent Profile Designed for C2S application and associated access control solutions*
- *CDS Services v1.0 Draft*

- HL7.org Standards: www.hl7.org

Current eHealth Exchange Specifications

- *Web Services Registry Web Service Interface Specification V3.1*
- *Patient Discovery Web Service Interface Specification V2.0*
- *Messaging Platform Specification V 3.0*
- *Authorization Framework Specification V 3.0*
- *Query for Documents Web Service Interface Specification V 3.0*
- *Retrieve Documents Web Service Interface Specification V 3.0*
- *Document Submission Production Web Service Interface Specification V 2.0*

Current Carequality Specifications

- *Query-Based Document Exchange Implementation Guide V 1.1*
- *Technical Trust Policy V1.2*

Current Commonwell Specifications

- *CommonWell Health Alliance Services Specification Version 2.9.1*

Joint DoD/VA Interoperability Plans and Processes

- Health Data Interoperability Management Plan v 3.0: DoD/VA Interagency Program Office, September 14, 2016.
- 2. Healthcare Information Interoperability Technical Package (I2TP) v 6.0: DoD/VA Interagency Program Office, March 15, 2017.
- Joint Interoperability Strategic Plan (JISP) v1.0: DoD/VA Interagency Program Office, September 30 2017.

6.0 Deliverables

6.1 Products

All products shall be delivered to the Government locations and accepted by authorized Government personnel as specified in the individual TO. Inspection and acceptance criteria shall be specifically identified in each TO. The COR shall be notified of any discrepancies found during acceptance inspection upon identification.

6.2 Data

If identified in an applicable Task Order, the Government shall receive Unlimited Rights to intellectual property first produced, and delivered in the performance of this contract IAW FAR 52.227-14, Rights In Data-General (DEC 2007). This includes all rights to source code and any and all documentation created in support thereof. For sake of clarity, this does not include minor modifications made to Contractor's Commercial Computer Software.

For all other commercial computer software licensed under this contract, the License rights in any Commercial Computer Software shall be governed by FAR 52.227-19, Commercial Computer Software License (DEC 2007) and the Contractor's or applicable supplier's End User License Agreement.

7.0 Information Security, Privacy And Records Management

In the EHRM and HA CAS environments (as defined in the Hosting Scope document), the Contractor shall comply with VA security, privacy and records management policies, directives, handbooks, and guidelines except where there is a conflict with DoD security, privacy and records management policies, directives, handbooks, and guidelines, in which case, joint governance will provide guidance to the Contractor. VA data stored within the Cerner security boundary shall be protected by the Contractor in compliance with VA security, privacy and record management policies as defined below. For VA data utilizing commercial solutions and service providers in the CAS and VAN services environment and in transit inside and outside the Cerner security boundary, the commercial solutions and service providers in the CAS and VAN services environments will comply with HIPAA and applicable Business Associate Agreement obligations. For clarity, such commercial service providers are not subject to the requirements set forth in this Section 7 of the PWS or the associated cybersecurity requirements set forth in the RTM.

7.1 VA Information And Information System Security / Privacy Language

7.1.1 General

Contractors, Contractor personnel, Subcontractors, and Subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

The Contractor shall comply with the RTM System security requirements for EHRM processing and infrastructure, both at the hosting facility and application level as well as additional security requirements agreed upon by the Joint Governance Committee.

7.1.2 Access To VA Information And VA Information Systems

a) A Contractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, Subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or TO.
b) Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or

mandates (e.g. Business Associate Agreement, Section 3G), the Contractor/ Subcontractor requires the joint governance approval.

c) The Contractor or Subcontractor must notify the Contracting Officer as soon as practical when an employee working on a VA system or with access to VA information is reassigned or leaves the Contractor or Subcontractor's employ.

d) The Contracting Officer must be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.

7.1.3 **VA Information Custodial Language**

a) Information made available to the Contractor or Subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of VA. This clause expressly limits the Contractor/Subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).

b) VA information should not be co-mingled, if possible, with any non-IPO approved data on the Contractors/Subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the Contractor must ensure that VA's information is returned to VA or destroyed in accordance with NIST sanitization requirements. VA reserves the right to conduct onsite inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with NIST requirements.

c) Prior to termination or completion of this contract, Contractor/Subcontractor must not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by VA. Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA Contracting Officer within 30 days of termination of the contract.

d) The Contractor/Subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after

execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

e) The Contractor/Subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on Contractor/Subcontractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor/Subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

f) If VA determines that the Contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the Contractor or third party.

g) If a VHA contract is terminated for cause, the associated Business Associate Agreement (BAA) must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.05, Business Associate Agreements. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

h) The Contractor/Subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using FIPS 140-2 compliant solutions.

i) The Contractor/Subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed NIST requirements.

j) Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor/Subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA's prior written approval. The Contractor/Subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA contracting officer for response.

k) Notwithstanding the provision above, the Contractor/Subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus, except as required by court or administrative tribunal order. If the Contractor/Subcontractor is in receipt of a court or

administrative tribunal order or other requests for the above mentioned information, that Contractor/Subcontractor shall immediately refer such court orders or other requests to the VA contracting officer for response.

l) For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require Assessment and Authorization (A&A) or a Memorandum of Understanding-Interconnection Security Agreement (MOU-ISA) for system interconnection, the Contractor/Subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

7.1.4 **Security Incident Investigation**

The Contractor shall:

a) Provide an Incident Management Plan for VA COR review and concurrence
b) Execute the activities identified in the approved Incident Management Plan
c) Analyze incidents and report results in a Technical Report to the EHRM PMO

The Contractor shall inform the IPO Incident Response POCs (System Owner, ISO, Privacy Officer, etc.) of information security & privacy incidents or adverse events for coordination of formal agency incident response processes. Federal law requires Federal agencies to report incidents to the United States Computer Emergency Readiness Team (US-CERT) office within the Department of Homeland Security (DHS). The Contractor shall follow the US-CERT Federal Incident Notification Guidelines (https://www.us-cert.gov/incident-notification-guidelines).

For the purposes of this PWS, an incident is defined as an occurrence that jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processing & computing, storage, or transmission or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies, such as, but not limited to Service Provider SLAs, Service Provider “Corporate” security policies, and Agency data sharing agreements. The Contractor is not required to notify VA of unsuccessful security incidents which include, but are not limited to, pings and other broadcast attacks on Contractor’s firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in known loss of confidentiality, integrity or availability of the EHRM system.

The Contractor shall coordinate with DoD to provide VA access to cyber-security incident and event logs for analysis. The Contractor’s EHRM hosting boundaries & DoD/VA EHR application virtual private network environments are within scope of incident reporting and event logs.

a) To the extent known by the Contractor, the Contractor’s notice to VA shall identify the information involved, the circumstances surrounding the incident

(including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the contractor/subcontractor considers relevant.

b) With respect to unsecured protected health information, the Contractor is deemed to have discovered a data breach when the Contractor knew or should have known of a breach of such information. Upon discovery, the Contractor must notify the VA of the breach. Notifications need to be made in accordance with the executed business associate agreement.

c) In instances of theft or break-in or other criminal activity, the Contractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The Contractor, its employees, and its subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

The Contractor shall cooperate with authorized Government offices in the areas of facilities access, audits, security incident notification, and hosting location. Specifically, the Contractor (and any Subcontractors) shall:

a) Provide the CO, designated representative of the CO, and representatives of authorized Government offices, supervised physical and logical access to the Contractor's (and Subcontractors') facilities, installations, operations documentation, databases, and personnel used for contract hosting services; provided the VA provides no less than ten business days prior notice to Contractor of its requested access unless at directed request from OIG This access shall be provided to the extent required to carry out audits, inspections, device scanning utilizing Government prescribed tools in accordance with the RTM, investigations, or other reviews to ensure compliance with contractual requirements for IT and information security, and to safeguard against threats and hazards to the integrity, availability, and confidentiality of agency information in the possession or under the control of the Contractor (or Subcontractor)

b) Fully cooperate with all audits, inspections, investigations, or other reviews conducted by or on behalf of the CO or other authorized Government offices as described in subparagraph (a) as described above. Full cooperation includes, but is not limited to, prompt disclosure (per agency policy) to authorized requests of data, information, and records requested in connection with any audit, inspection, investigation, or review, making employees of the Contractor available for interview by auditors, inspectors, and investigators within ten business days from such request unless at the direct request from OIG. The Contractor shall, provide access (per agency policy) to Contractor facilities, systems, data and personnel to the extent the auditors, inspectors, and investigators reasonably believe necessary to complete the audit, inspection, investigation, or other

review. The Contractor's (and any Subcontractors') cooperation with audits, inspections, investigations, and reviews conducted under this clause will be provided at no additional cost to the Government. Per the Inspector General Act of 1978, the Contractor shall:

i. Provide full and unfettered logical access to VA application, system and audit logging data based on joint governance approval. The documentation must be provided to OIG personnel at no cost to OIG and contemporaneous to being requested by OIG;
ii. Retain audit logs for a minimum of 1 year or as documented in the NARA retention periods, HIPAA legislation (for VHA), or whichever is greater. Audit logs which describe a security breach must be maintained for 6 years (HIPAA requirement);
iii. Allow VA OIG access to collect any and all VA data directly from the Managed Services Provider, without the need to coordinate access or notify any 3rd party provider/facilitator;
iv. Ensure that VA Systems and data hosted with a Managed Services Provider must be encrypted both in transit and at rest to adequately protect sensitive veteran information; and,

c) Preserve such data, records, logs and other evidence which are reasonably necessary to conduct a thorough investigation of any computer security incident.
d) Promptly notify the designated agency representative in the event of any computer security and privacy incident as described in paragraph (c) above. This notification requirement is in addition to any other notification requirements which may be required by law or this contract. Established Federal agency timeframes for reporting security and privacy incidents to the United States Computer Emergency Readiness Team (US-CERT), although not exhaustive, serve as a useful guideline for determining whether reports under this paragraph are made promptly. (See NIST SP 800-61, Computer Security Incident Handling Guide, Appendix J)
e) Provide to the requestor (CO, a representative of the CO, or authorized Government offices) Government data, information, or records under the control of or in the possession of the Contractor pursuant to this contract, which the Agency or authorized Government offices, including the OIG, may request in furtherance of other audits, inspections, investigations, reviews or litigation in which the Agency or other authorized Government offices are involved in the form specified at the TO level. Requests for production under this paragraph shall specify a deadline not less than ten days for compliance which will determine whether response to the request has been made in a timely manner. Unless expressly provided otherwise elsewhere in this contract, the production of data, information, or records under this paragraph will be at no additional cost to the Government
f) Include the substance of this Section, including this paragraph (f) in any subcontract which would require or otherwise result in Subcontractor employees having access to agency information in the possession or under the control of the Subcontractor, or access to information systems operated by the Subcontractor in the performance of this contract

g) Ensure that all hosting services pertaining to this contract are performed within the United States of America, including the storage of agency data, information, and records under the control of or in the possession of the Contractor pursuant to this contract
h) Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates (e.g. Business Associate Agreement, Section 3G), the Contractor/ Subcontractor requires the IPO approval.

7.1.1 **Security Controls Compliance Testing**

On an annual basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the Contractor under the clauses contained within the contract in coordination with the DoD or joint governance entity. With 10 working-days' notice, at the request of the Government in coordination with the DoD or joint governance entity,, the Contractor must fully cooperate and assist in a Government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The Government may conduct a security control assessment on shorter notice as determined by VA in the event of a security incident in coordination with the DoD or joint governance entity.

7.1.2 **Training**

a. **Security And Privacy Awareness Training**

The Contractor's employees shall complete the initial agreed upon Privacy and Information Security Awareness and Rules of Behavior (TMS# VA10176) and Privacy and HIPAA Training (TMS# VA10203) within thirty business days of onboarding in the VA Talent Management System (TMS). If training from the Department of Defense is provided, the VA COR will track the DoD training status, retain copies of completion certificates and communicate with the VA TMS administrator to keep TMS expiration dates consistent. The Contractor shall renew these trainings annually prior to expiration in the VA TMS.

b. **Security Role Based Training**

The Contractor shall complete the assigned security role-based training and provide completion certificates within ten business days of COR identification of need for privileged access to VA-managed systems. The Contractor and the VA will mutually agree to the mapping of the roles. The following are required for the specific elevated privileged roles:

i. TMS #3197 – Information Security Role-Based Training for IT Specialist
ii. TMS #3867207 – Information Security Role-Based Training for System Owners
iii. TMS #1016925 – Information Security Role-Based Training for Software Developers
iv. TMS #1357076 – Information Security Role-Based Training for System Administrators
v. TMS #1357084 – Information Security Role-Based Training for Data Manager
vi. TMS #1357083 – Information Security Role-Based Training for Network Administrators
vii. TMS #64899 – Information Security Role-Based Training for IT Project Managers

c. Failure to complete the mandatory annual training and electronically sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

7.2 PRIVACY / SYSTEMS OF RECORD

7.2.1 Systems of Record

The Contractor/Subcontractor is required to design, develop, or operate a System of Records Notice (SORN) on individuals to accomplish an agency function subject to the Privacy Act of 1974, (as amended), Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Privacy Act may involve the imposition of criminal and civil penalties.

The Contractor/Subcontractor agrees to:

1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies:

(a) The Systems of Records (SOR); and

(b) The design, development, or operation work that the Contractor/Subcontractor is to perform;

2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a SOR on individuals that is subject to the Privacy Act; and

3) Include this Privacy Act clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a SOR

4) In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a SOR on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a SOR on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a SOR on individuals to accomplish an agency function, the Contractor/Subcontractor is considered to be an employee of the agency.

5) "Operation of a System of Records" means performance of any of the activities associated with maintaining the SOR, including the collection, use, maintenance, and dissemination of records.

6) "Record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and contains the person's name, or identifying number, symbol, or any other identifying particular assigned to the individual, such as a fingerprint or voiceprint, or a photograph.

7) "System of Records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The service provider shall notify the Designated Government Official within the authorizing agency's specified timeframe of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality, integrity or availabilityof its data, operations, or the system). Such issues shall be remediated in accordance with the Designated Government Official established continuous monitoring requirements. When the Security Fixes involve installing patches the service provider will inform the Designated Government Official within 10 working days.

When the vendor is responsible for operations or maintenance of the Systems, they shall apply the Security Fixes within the authorizing agency's specified timeframe.

7.2.1 **Confidentiality and Non-Disclosure**

a) The Contractor shall follow all applicable VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations to the extent that they are consistent with the analogous MHS GENESIS rules and regulations.

b) The Contractor may have access to Protected Health Information (PHI) and Electronic Protected Health Information (EPHI) that is subject to protection under the regulations issued by the Department of Health and Human Services, as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA); 45 CFR Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule"); and 45 CFR Parts 160 and 164, Subparts A and C, the Security Standard ("Security Rule"). Pursuant to the Privacy and Security Rules, the Contractor must agree in writing to certain mandatory provisions regarding the use and disclosure of PHI and EPHI. These mandatory provisions will be set forth in the business associate agreement.

c) The Contractor will have access to some privileged and confidential materials of VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of VA. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.

d) The VA Contracting Officer will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information. Any request for information relating to this contract presented to the Contractor shall be submitted to the VA Contracting Officer for response.

e) Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.

f) Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the Contractor has a responsibility to ask the VA Contracting Officer.

g) Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.

h) Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security

procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA Contractor shall adhere to the following:

i. The use of “thumb drives” or any other medium for transport of information is expressly prohibited.
ii. Controlled access to system and security software and documentation.
iii. Recording, monitoring, and control of passwords and privileges.
iv. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
v. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
vi. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".

i) Contractor may require access to classified data.

j) Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.

7.2.2 **Liquidated Damages For Data Breach**

a) Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the Contractor may be liable to VA for liquidated damages in the event of a data breach involving any SPI the Contractor/Subcontractor processes or maintains under this contract to the extent that such breach is the result of the Contractor’s error or omission. However, it is the policy of VA to forgo collection of liquidated damages in the event the Contractor provides payment of actual damages in an amount determined to be adequate by the agency.

b) The Contractor shall provide notice to VA of a data breach as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the

entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

c) Each risk analysis shall address all relevant information concerning the data breach, including the following:

i. Nature of the event (loss, theft, unauthorized access);
ii. Description of the event, including:
    1. date of occurrence;
    2. data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
iii. Number of individuals affected or potentially affected;
iv. Names of individuals or groups affected or potentially affected;
v. Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;
vi. Amount of time the data has been out of Contractor's control;
vii. The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
viii. Known misuses of data containing sensitive personal information, if any;
ix. Assessment of the potential harm to the affected individuals;
x. Data breach analysis as outlined in 6500.2 Handbook, *Management of Breaches Involving Sensitive Personal Information*, as appropriate; and
xi. Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

d) Based on the determinations of the independent risk analysis, if the Contractor does not pay actual damages, then the Contractor shall be responsible for paying to VA liquidated damages in the amount of $37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

i. Notification;
ii. One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
iii. Data breach analysis;
iv. Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;

v. One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and
vi. Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

7.3 RECORDS MANAGEMENT

a) The Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. chs. 21, 29, 31, 33), NARA regulations at 36 CFR Chapter XII Subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all records, regardless of form or characteristics, mode of transmission, or state of completion. Contractor shall return all applicable records to the Government upon termination of the EHRM remote hosting services.

b) In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), as amended, and the Privacy Act of 1974 (5 U.S.C. 552a), as amended and must be managed and scheduled for disposition only as permitted by statute or regulation.

c) In accordance with 36 CFR 1222.32, Contractor shall maintain all records created for Government use or created in the course of performing the contract and/or delivered to, or under the legal control of the Government and must be managed in accordance with Federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.

d) The Contractor is responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Records may not be removed from the legal custody of VA or destroyed except for in accordance with the provisions of the agency records schedules and with the written concurrence of the Head of the Contracting Activity. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701.

e) In the event of any unlawful or accidental removal, defacing, alteration, or destruction of records, Contractor must report to VA. The agency must report promptly to NARA in accordance with 36 CFR 1230.

7.3.1 Flowdown Of Requirements To Subcontractors

a) The Contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all applicable subcontracts.

b) Violation by a subcontractor of any provision set forth in this clause will be attributed to the Contractor.

8.0 General Requirements

8.1 Materials, Equipment And Locations

8.1.1 Government-Furnished and Connectivity

Government Furnished Property (GFP) which includes Government Furnished Material (GFM), Government Furnished Information (GFI), and GFE may be provided and shall be identified in the individual TO. The Contractor shall be responsible for conducting all necessary examinations, inspections, maintenance, and tests upon receipt. The Contractor shall be responsible for reporting all inspection results, maintenance actions, losses, and damage to the Government. Should any property be lost, stolen or destroyed due to Contractor's negligence, the Contractor is responsible for replacing the property. The Contractor may be provided keys or codes for access to a Government facility during individual TO performance. These keys and codes shall be controlled, tracked, and protected. Upon completion of the TO period of performance, all keys and/or access badges to the Government facility shall be turned in to the VA PM or COR.

VA may provide VA specific software as appropriate and required in individual TOs. The Contractor may utilize VA provided software development and test accounts, document and requirements repositories and others as required for the development, storage, maintenance and delivery of products. Contractors shall comply with VA security policies and procedures with respect to protecting sensitive data. See Section 7.0 for detailed security requirements.

VA may provide remote access to VA specific systems/network in accordance with VA Handbook 6500, which requires the use of a VA approved method to connect external equipment/systems to VA's network. For the sake of clarity, this does not include access to MHS Genesis or to Contractor's environment. Citrix Access Gateway (CAG) is the current and only VA approved method for remote access users when using or manipulating VA information for official VA Business. VA permits CAG remote access through approved Personally Owned Equipment (POE) and Other Equipment (OE) provided the equipment meets all applicable 6500 Handbook requirements for POE/OE All of the security controls required for Government furnished equipment (GFE) must be utilized in approved POE or OE. The Contractor shall provide proof to the COR for review and approval that their POE or OE meets the VA Handbook 6500 requirements and VA Handbook 6500.6 Appendix C, herein incorporated as Addendum B, before use. CAG authorized users shall not be permitted to copy, print or save any VA

information accessed via CAG at any time. VA prohibits remote access to VA's network from non-North Atlantic Treaty Organization (NATO) countries. The exception to this are countries where VA has approved operations established (e.g. Philippines and South Korea). Exceptions are determined by the COR in coordination with the Information Security Officer (ISO) and Privacy Officer (PO).

This remote access may provide access to VA specific software such as VistA, ClearQuest, ProPath (PAL), Primavera, Rational, and service desk software. including appropriate seat management and user licenses, depending upon the level of access granted. The Contractor shall utilize government-provided software development and test accounts, document and requirements repositories, etc. as required for the development, storage, maintenance and delivery of products within the scope of this effort. The Contractor shall not transmit, store or otherwise maintain sensitive data or products in Contractor systems (or media) outside of the MHS Genesis hosting environment IAW VA Handbook 6500.6 dated March 12, 2010. All VA sensitive information shall be protected at all times in accordance with RTM.

VA will provide connectivity to VA specific systems/network as required for execution of the task via VA approved remote access technology. Currently this may include but is not limited to CAG, site-to-site virtual private network (VPN), or VA Remote Access Security Compliance Update Environment (RESCUE). This remote access will provide connectivity to VA specific software such as VistA, ClearQuest, ProPath (PAL), Primavera, Rational, and VA service desk software, including appropriate seat management and user licenses. VA may install equipment at the Contractor's site to ensure security requirements are in place. The Contractor must meet the requirements of VA Handbook 6500 and will bear the cost to provide connectivity to VA. Other connectivity to VA systems may be authorized as appropriate in individual TOs.

8.1.2 **Contractor-Acquired Property**

The Contractor shall acquire and/or provide any hardware and/or software required to accomplish each TO that is not provided as GFP. Software integrity shall be maintained by the Contractor within the licensing agreement of the producer until such software is delivered to the Government, or otherwise disposed of IAW Government direction. Items delivered to the Government shall be approved by the Government in advance of purchase and shall be in compliance with VA requirements.

8.1.3 **Non-Developmental Items and Commercial Processes**

Non-Developmental Items (NDI), Commercial-Off-The-Shelf (COTS) and Government-Off-The-Shelf (GOTS) products shall be used to the maximum extent. The Contractor shall apply commercially available and industry best processes, standards and technologies to the maximum extent.

8.1.4 **Facilities**

Work may be performed at either a Government or non-Government facility. Each TO shall delineate the location requirements.

8.1.4.1 **Government Facilities**

Certain Government office or laboratory space may be made available for performance of individual TOs. Contractors may be required to establish operations and support Government locations and shall comply with VA and/or Federal A&A requirements. Such facilities shall be specified in the individual TO.

8.1.4.2 **Non-Government Facilities**

Personnel may perform at Contractor or remote facilities if specified in the individual TO. Contractors may be required to establish operations and support Contractor facilities and shall comply with RTM system access requirements. Such facilities shall be specified in the individual TO. The Contractor shall disclose specific facility information during the Request for Task Execution Plan (RTEP) process.

8.1.5 **Warranty**

Items acquired under this contract may require warranty protection. Commercial warranties shall be transferred to the Government. The type of warranty and extent of coverage shall be determined on an individual TO basis.

8.1.6 **Marking, Handling, Storage**, **Preservation, Packaging, Tracking & Shipping**

The Contractor shall establish/maintain procedures IAW VA Handbook 6500 and VA Directive 6609 for handling, storage, preservation, packaging, marking, tracking and shipping to protect the quality of products and prevent damage, loss, deterioration, degradation or substitution of products.

8.1.7 **Export Control**

The Contractor shall comply with all applicable laws and regulations regarding export-controlled information and technology and shall not use, distribute, transfer or transmit technology (even if incorporated into products, software or other information) except in compliance with such laws and regulations. In addition, the Contractor shall plan for, obtain, and maintain any and all export licensing required to satisfy individual TO requirements.

8.2 **Safety And Environmental**

Safety and environmental procedures shall be identified in individual TO requirements.

The Contractor shall comply with the Office of Federal Procurement Policy Green Acquisition initiatives as identified in individual TO.

8.3 Enterprise And IT Framework

Enterprise and IT Framework provisions apply only to any Cerner-developed VA-owned software that will reside on the VA network. This does not include development on Cerner COTS platforms such as: Millennium, HealtheIntent, and CareAware.

In association with the framework, the Contractor shall comply with OI&T Technical Reference Model (One-VA TRM) and consider the OneVA Enterprise Technology Strategic Plan. One-VA TRM is one component within the overall Enterprise Architecture (EA) that establishes a common vocabulary and structure for describing the IT used to develop, operate, and maintain enterprise applications.

The Contractor shall ensure COTS product(s), software configuration and customization, and/or new software are PIV-enabled by accepting HSPD-12 PIV credentials using VA Enterprise Technical Architecture (ETA), http://www.ea.oit.va.gov/VA_EA/VAEA_TechnicalArchitecture.asp, and VA Identity and Access Management (IAM) approved enterprise design and integration patterns, http://www.techstrategies.oit.va.gov/enterprise_dp.asp. The Contractor shall ensure all Contractor delivered applications and systems are compliant with VA Identity Management Policy (VAIQ# 7011145), Continued Implementation of Homeland Security Presidential Directive 12 (VAIQ#7100147), and VA IAM enterprise identity management requirements (IAM Identity Management Business Requirements Guidance document), located at https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514.. The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with NIST Special Publication 800-63, VA Handbook 6500 Appendix F, “VA System Security Controls”, and VA IAM enterprise requirements for direct, assertion based authentication, and/or trust based authentication, as determined by the design and integration patterns. Direct authentication at a minimum must include Public Key Infrastructure (PKI) based authentication supportive of PIV and/or Common Access Card (CAC), as determined by the business need. Assertion based authentication must include a SAML implementation. Additional assertion implementations, besides the required SAML assertion, may be provided as long as they are compliant with NIST 800-63 guidelines. Trust based authentication must include authentication/account binding based on trusted HTTP headers. The Contractor solution shall conform to the specific Identity and Access Management PIV requirements set forth in OMB Memoranda M-04-04, M-05-24, M-11-11, as well as the NIST FIPS 201-2, and supporting NIST Special Publications. OMB Memoranda M-04-04, M-05-24, and M-11-11 can be found at: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy04/m04-04.pdf, https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-24.pdf, and https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2011/m11-

11.pdf respectively. The identity authentication Level of Assurance (LOA) requirement is LOA-4 unless otherwise specified at the TO level.

The Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) based upon the directives issued by the OMB on August 2, 2005 (https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf) and September 28, 2010 (https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf).). IPv6 technology, in accordance with the USGv6 Profile (NIST Special Publication (SP) 500-267 (http://www-x.antd.nist.gov/usgv6/index.html), the Technical Infrastructure for USGv6 Adoption (http://www.nist.gov/itl/antd/usgv6.cfm), and the NIST SP 800 series applicable compliance (http://csrc.nist.gov/publications/PubsSPs.html) shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. In addition to the above requirements, all devices shall support native IPv6 and/or dual stack IPv6 IPv4 connectivity without additional memory or other resources being provided by the Government, so that they can function in a mixed environment. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) shall support native IPv6 and/or dual stack IPv6 IPv4 users and all internal infrastructure and applications shall communicate using native IPv6 and/or dual stack IPv6 IPv4 operations. Guidance and support of improved methodologies which ensure interoperability with legacy protocol and services in dual stack solutions, in addition to OMB/VA memoranda, can be found at: https://www.voa.va.gov/documentlistpublic.aspx?NodeID=282.

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M08-05 mandating Trusted Internet Connections (TIC) (https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf), M08-23 mandating Domain Name System Security (NSSEC) (https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-23.pdf), and shall comply with the TIC Reference Architecture Document, Version 2.0 https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/04/TIC_Ref_Arch_v2-0_2013.pdf.
), M08-23 mandating Domain Name System Security (NSSEC) (), and shall comply with the TIC Reference Architecture Document, Version 2.0.

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating system, currently Windows 7 (64bit), (with Windows 10 and Edge scheduled for deployment in 2018), Internet Explorer 11 and Microsoft Office 2010. In preparation for the future VA standard configuration update, end user solutions shall also be compatible with Office 2013, and Windows 8.1. Upon the release approval of Office 2013, and Windows 8.1 individually as the VA standard, Office 2013, and Windows 8.1 will supersede Office 2010 and Windows 7 respectively. Applications delivered to the VA and intended to be deployed to Windows 7 workstations shall be delivered as a signed .msi package and updates shall be delivered in signed .msp file formats for easy deployment using System Center Configuration Manager (SCCM) VA's current desktop

application deployment tool. Signing of the software code shall be through a vendor provided certificate that is trusted by the VA using a code signing authority such as Verizon/Cybertrust or Symantec/VeriSign. The Contractor shall also ensure and certify that their solution functions as expected when used from a standard VA computer, with non-admin, standard user rights that have been configured using the United States Government Configuration Baseline (USGCB) specific to the particular client operating system being used.

The Enterprise Management Framework (EMF) provides an enterprise-wide view of VA IT systems comprised of tools, reports, databases, dashboards, and analytics. EMF supports a unified enterprise service management model including release management, configuration management, change management, and incident management aligned with industry standard IT Infrastructure Library (ITIL) service management best practices. The EMF Federated Data Repository (FDR) includes the implementation of a foundational component. The EMF FDR is a national repository that collects enterprise IT management data from VA Managed Data Repositories (MDRs) and integrates with existing VA monitoring and performance systems.

Additional frameworks may be specified in individual TOs.

8.4 **Development Methodologies**

For custom interface development, the Contractor shall follow VA VIP major program processes in Section D Attachments 009 and 010 as required. ProPath processes will be made available to the Contractor for use if needed.

8.5 **Integrated Product Teams**

The Contractor may be required to serve as a member of, or provide Subject Matter Expertise to IPTs or Integrated Business Teams (IBTs) within VA. Their role(s) will be identified in individual TOs. IPTs and IBTs are cross-functional teams that work collaboratively to develop strategies and approaches to meet particular objectives. IPTs and IBTs bring together the principal stakeholders and focus efforts on establishing critical elements of all phases of the acquisition lifecycle.

8.6 **Quality Assurance**

Cerner will use its commercial Cerner Quality System (CQS) quality system with respect to the software and solutions delivered under this contract. CQS is Cerner's total systems approach to quality and is designed to build on the Food and Drug Administration's (FDA) Quality System Regulation (QSR) and the International Organization for Standardization's (ISO) quality management systems requirements (ISO 9001 for general quality management, and ISO 13485 for quality management specific to medical devices) for the purpose of ensuring quality throughout Cerner.

The Cerner Quality System (CQS) is a quality management system that fulfills the 21 CFR Part 820 Quality System Regulations and is based on the commitment to achieving safety and effectiveness of solutions and services in the interest of the public health and in the interest of each client. CQS establishes how Cerner shall embody quality throughout the lifecycles of the solutions and services it provides. CQS is a dynamic system and is intended to remain so through continuous feedback, monitoring by system audits, management review, and corrective and preventive action. CQS is continuously improved through formal change management and document control processes, requiring review and approval at executive levels.

Additionally, a basic and individual task order Quality Assurance Surveillance Plans (QASPs) will be utilized throughout the life of the contract/order to ensure that the Contractor is performing the services required by the PWS at an acceptable level of performance. The Government reserves the right to alter or change the QASPs at its own discretion. Contractor performance and reporting requirements as they pertain to the basic QASP are defined in this PWS and accompanying attachments such as the Requirements Traceability Matrix (RTM), Software Assurance Standard Operating Procedure, and Veteran-Focused Integration Process (VIP) Major Program Deployment Guide. Additionally, Functional and Non-Functional Key Performance Indicators (KPIs) are defined in Appendix A of the basic QASP. The Government may also utilize Cerner's commercially available KPIs and Service Level Agreements (SLAs) to monitor and measure Contractor performance. Contractor performance and reporting requirements will be further defined for individual task order requirements. Additional KPIs may also be defined at later dates for individual task order requirements, or at the ID/IQ level as approved through EHRM governance boards, as needed and as determined by the government in accordance with the organization's mission. Copies of the basic and individual task order QASPs and revisions shall be provided to the Contractor and Government officials responsible for surveillance activities. The Government can change the method of surveillance at any time without the approval of the contractor.

8.7 **Personnel Security Requirements**

The Contractor(s) shall comply with all personnel security requirements included in this contract and any unique organization security requirements described in each TO. All Contractor personnel who require access to VA sensitive information/computer systems shall be subject to background investigations and must receive a favorable background investigation from VA.

The position sensitivity risk designation [LOW, MODERATE, and HIGH] and associated level of background investigation [Tier 1, Tier 2, and Tier 4] for each TO PWS task shall be designated accordingly, as identified within Section 4.6 of the TO PWS. VA will apply reciprocity to existing DoD background investigations, as long as there has not been a break in service of 24 months, and the investigation meets or exceeds what is

required. The Contractor shall provide name, SSN, date of birth, place of birth and DoD background investigation date and number in order to determine reciprocity. For VA-conducted background investigations, the level and process of background security investigations for Contractors must be IAW VA Directive and Handbook 0710, "Personnel Security and Suitability Program".

a. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language.
b. The Contractor shall perform electronic fingerprinting onsite using a VA mobile facility if available, or coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized. The Contractor shall bring their completed Security and Investigations Center (SIC) Fingerprint request form with them (see paragraph d.4 below) when getting fingerprints taken
c. The Contractor shall ensure the following required forms are submitted to the COR within thirty days after an employee is resourced to the project:
    1) Optional Form 306
    2) Self-Certification of Continuous Service
    3) VA Form 0710
    4) SIC Fingerprint Request Form
    5) Contractor Background Investigation (CBIR)Form
    6) Special Agreement Check (SAC) Form
    7) Training Management Service (TMS) Form
    8) EHRM Non-Disclosure Agreement (NDA)
d. The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the SIC.
e. The Contractor employee shall certify and release the e-QIP document, print and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within three business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a "click to sign" process. If click to sign is used, the Contractor employee should notify COR within three business days that documents were signed via eQIP).
f. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.
g. If the background investigation determination is not completed prior to the start date of work identified in each TO, a Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement

Check (SAC), completed training delineated in VA Handbook 6500.6 (Appendix C, Section 9), signed “Contractor Rules of Behavior”, and with a valid, Government-approved ID operational PIV credential for PIV-only logical access to VA’s network. A PIV card credential can be issued once your SAC has been favorably adjudicated and your background investigation has been scheduled by OPM. However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of the OPM.

h. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.
i. Failure to comply with the Contractor personnel security investigative requirements may result in loss of physical and/or logical access to VA facilities and systems by Contractor and Subcontractor employees, and in extreme cases termination of the contract for default.
j. Identity Credential Holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.

For efforts impacting DoD implementations, additional security clearance requirements will be identified at the TO level.

8.8 **Badges, Physical Security, and Safety Requirements**

Employees working at a Government facility may be required to display, on their person, a Government-provided identification badge, that shall include the full name of the employee and the legal name under which the Contractor is operating. It is the responsibility of the Contractor to request and obtain badges from the Government prior to the first workday on Government facility of any Contractor employee. If Contractor employee must visit a Government facility prior to receipt of badge, Contractor employee will follow on-site visitor requirements of Government facility. The Contractor shall return all badges to the COR, or designee, promptly upon an individual’s employment is terminated and upon termination of the contract. The Contractor shall notify the Government program manager, or designee, immediately of any lost badges.

The Contractor and their personnel shall follow all VA policies, standard operating procedures, applicable laws and regulations while on VA property. Violations of VA regulations and policies may result in citation and disciplinary measures for persons violating the law.

1. The Contractor and their personnel shall wear visible identification at all times while they are on the premises.
2. VA does not provide parking spaces at the work site; the Contractor must obtain parking at the work site if needed. It is the responsibility of the Contractor to park

in the appropriate designated parking areas. VA will not invalidate or make reimbursement for parking violations of the Contractor under any conditions.
3. Smoking is prohibited inside/outside any building other than the designated smoking areas.
4. Possession of weapons is prohibited.
5. The Contractor shall obtain all necessary licenses and/or permits required to perform the work, with the exception of software licenses that need to be procured from a Contractor or vendor in accordance with the requirements document. The Contractor shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract.

8.9 NOTICE OF THE FEDERAL ACCESSIBILITY LAW AFFECTING ALL INFORMATION AND COMMUNICATION TECHNOLOGY PROCUREMENTS (SECTION 508)

On January 18, 2017, revised and updated, in a single rulemaking, standards for electronic and information technology developed, procured, maintained, or used by Federal agencies covered by section 508 of the Rehabilitation Act of 1973, as well as our guidelines for telecommunications equipment and customer premises equipment covered by Section 255 of the Communications Act of 1934. The revisions and updates to the section 508-based standards and section 255-based guidelines are intended to ensure that information and communication technology covered by the respective statutes is accessible to and usable by individuals with disabilities.

8.10 SECTION 508 – INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) STANDARDS

The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Information and Communication Technology (ICT). These standards are found in their entirety at: http://www.section508.gov and https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule/text-of-the-standards-and-guidelines. A printed copy of the standards will be supplied upon request.

The Access Board updated the Section 508 standards on January 18, 2017. The updated standards are effective on March 21, 2017. The Final Rule as published in the Federal Register is available from the Access Board: https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule.

The Contractor shall comply with the Scoping Requirements for all electronic ICT and content delivered under this contract.

8.10.1 **Compatibility With Assistive Technology**

The standards do not require installation of specific accessibility-related software or attachment of an assistive technology device, but require that ICT be compatible with such software and devices so that it can be made accessible if so required by the agency in the future. Section 508 requires that ICT be compatible with such software and devices so that ICT can be accessible to and usable by individuals using assistive technology, including but not limited to screen readers, screen magnifiers, and speech recognition software.

8.10.2 **Equivalent Facilitation**

Alternatively, offerors may propose products and services that provide equivalent facilitation, pursuant to Section 508, E101.2. Such offerors will be considered to have provided equivalent facilitation when the proposed deliverables result in substantially equivalent or greater access to and use of information for those with disabilities.

The Section 508 standards do not require installation of specific accessibility-related software or attachment of an assistive technology device.

8.10.3 **Representation Of Conformance**

Products should include test results or other conformance statements validating conformance to the Section 508 Refresh Success Criteria and Conformance Requirements.

8.10.4 **Acceptance And Acceptance Testing**

Deliverables resulting from this solicitation will be accepted based in part on satisfaction of the identified Section 508 standards' requirements for accessibility and must include a final updated GPAT or VPAT.

Deliverables should meet applicable accessibility requirements and should not adversely affect accessibility features of existing ICT technologies. The Government reserves the right to independently test for 508 Compliance before delivery. The Contractor shall be able to demonstrate 508 Compliance upon delivery.

9.0 CONTRACT MANAGEMENT

9.1 **CONTRACTOR PROGRAM MANAGEMENT**

The Contractor shall establish a single management focal point, the Program Manager, to accomplish the administrative, managerial and financial aspects of this contract and

all subsequent TOs. This individual shall be identified to the TAC as the focal point for all programmatic issues.

9.1.1 **Work Control**

All program requirements, contract actions and data interchange shall be conducted in a digital environment using electronic and web-based applications. At minimum, such data shall be compatible with the Microsoft Office 2010® family of products, Microsoft Windows 7 products, Adobe Portable Document Format (PDF) and AutoCAD. The Government will designate a standard naming convention for all electronic submissions within 60 days after contract award.

9.2 **GOVERNMENT SUPPORT**

9.2.1 **Government Task Leader**

The Government Task Leader) GTL is the Requiring Activity's designated onsite representative. A GTL may be designated for each TO and is the COR's primary Point of Contact for managing the TO award and administration processes. The GTL will be appointed by the Contracting Officer and duties delegated in an appointment letter. The GTL shall coordinate performance assessment information with the COR, as well as keep adequate performance records to be included in the COR's quality assurance file. Only Government employees are permitted to be GTLs. The GTL is not empowered to make any contractual commitments or to authorize any contractual changes on the Government's behalf. Note: In coordination with the GTL or when a GTL is not designated for a particular TO, the VA Program Manager will assume these responsibilities.

9.2.2 **Contracting Officer's Representative (COR)**

A COR shall be designated for the ID/IQ and each individual TO. The COR will be appointed by the Contracting Officer and duties delegated in an appointment letter. The COR is responsible for technical administration of the contract/order and shall assure proper Government surveillance of the Contractor's performance. The COR shall keep a quality assurance file. This file shall contain all quality assessment reports. The COR is not empowered to make any contractual commitments or to authorize any contractual changes on the Government's behalf.

9.3 **PRE-AWARD PROCEDURES**

9.3.1 **Request for RTEP Process**

Upon identification of the need for a TO, a tracking number shall be assigned and the CO shall issue a RTEP to the Contractor. For Performance-Based tasks, the Government will specify requirements in terms of performance objectives. The

Contractor shall propose “how to” best satisfy those objectives including proposed metrics to measure and evaluate performance.

9.3.2 **Task Execution Plan (TEP)**

The Government’s RTEP does NOT constitute an authorization to start work.

Within seven work days of receipt of the RTEP, or unless otherwise specified in the RTEP, the Contractor shall submit one TEP in accordance with the format provided below unless otherwise specified by the CO. The following information shall be provided and submitted to VA:

A In addition to the information requested in the RTEP, the following shall be addressed in every TEP:
   1. Proposal Summary Volume including:
      a. Task number
      b. Date submitted
      c. Contractor’s name
      d. Contractor task leader contact information for questions
      e. Subcontractor(s) and vendors shall be identified by name at all tiers (as applicable)
      f. Proposed start and finish dates
      g. Proposed total price
      h. Offerors are hereby advised that any Offeror-imposed terms and conditions which deviate from the Government’s material terms and conditions established by the RTEP, may render the Offeror’s proposal Unacceptable, and thus ineligible for award.
      i. If applicable, FAR 52.244-2 Subcontracts shall be addressed
      j. Duration for which proposal is valid (minimum 90 days)
      k. VAAR 852.209-70 is in effect for all RTEPs issued and the contractor should provide a statement IAW VAAR 852.209-70(b), when applicable
      l. Acknowledgement of Amendments.
      m. Class Deviation from FAR 52.209-5 “Certification Regarding Responsibility Matters” applies for all issued RTEPS. The Contractor shall provide representation within the Summary Volume of its TEP.

   2 Service Contract Act price proposal volume shall be submitted in Microsoft Excel spreadsheet format. The first tab shall be a summary to include a top level rollup of the total dollars and percentages by labor, materials, travel, ODCs, and total TO price. Labor shall further be broken out by labor categories, labor rates, and hours. A separate tab shall be used for the Prime and each Subcontractor.

   3 The Contractor shall submit a completed Section B including all priced line items for the base period and any options.

   4 The Offeror are hereby advised that any Pricing Assumptions which deviate from the Government’s requirements or material terms and conditions established by

the RTEP, may render the Offeror's proposal Unacceptable, and thus ineligible for award.

5 The Offeror shall submit a draft Small Business Participation Report, to include identification of subcontractors, socio-economic categories, and estimated dollar values.

B The following pertains to the preparation and submission of all TEPs:

1 TEP Format

a Proposal Summary

i. Microsoft Word or PDF format

b Technical Volume

i Microsoft Word or PDF format

ii No marketing materials; information relevant to the requirement only

c Price

i. Shall be provided in Microsoft Excel

ii. All Prime and Subcontractor Labor costs, Material costs, Travel, and ODCs must be broken out

(a) (MS Excel) Summary Tab for Price roll-up, and separate Tabs for Base Period and any Option

(b) Separate tabs for Subcontractor(s)

2 Page Limitations. When page limitations are specified in the RTEP, the following format shall apply:

The Summary and Technical Volumes shall be submitted as a PDF file. Price Volume shall be submitted in Microsoft Excel. Page size shall be no greater than 8 1/2" x 11". The top, bottom, left and right margins shall be a minimum of one inch each. Font size shall be no smaller than 12-point. Times New Roman fonts are required. Characters shall be set at no less than normal spacing and 100% scale. Tables and illustrations may use a reduced font size not less than eight-point and may be landscape. Line spacing shall be set at no less than single space. Each paragraph shall be separated by at least one blank line (minimum six point line). Page numbers, company logos, and headers and footers may be within the page margins ONLY, and are not bound by the 12-point font requirement. Footnotes to text shall not be used. If the offeror submits annexes, documentation, attachments or the like, not specifically required by this solicitation, such will count against the offeror's page limitations unless otherwise indicated in the specific Volume instructions. Pages in violation of these instructions, either by exceeding the margin, font or spacing restrictions or by exceeding the total page limit for a particular volume, will not be evaluated. Pages not evaluated due to violation of the margin, font or spacing restrictions will not count against the page limitations. The page count will be determined by counting the pages in the order they come up in the print layout view. The Cover Page and Table of Contents are not included in the page count however any additional matrices, appendices, or acronym lists, etc. will count against page limitation. Cover letters shall not be included in the Technical Volume.

9.3.3 **TEP Evaluation**

The goal is to evaluate TEP submittals within 12 work days of receipt. Questions and clarifications may be required which can prolong the evaluation period. When requested by the CO, the Contractor shall provide a revised TEP to address changes.

9.4 **ISSUANCE OF TOS**

Upon Government approval of the TEP and designation of an appropriate fund cite, the CO shall issue a TO to the Contractor. Contractor work shall commence only after issuance of the TO by the CO.

9.5 **POST AWARD PROCEDURES**

9.5.1 **Request for Post Award Action**

Upon identification of the need for a modification to a TO, the Government shall issue a Request for Post Award Action, designated by an action number, to the Contractor. The CO shall designate individuals authorized to issue such requests upon TO award, in writing. The Contractor shall respond to requests from these authorized individuals only. All Contractor correspondence shall reference the Government designated action number. The Government's Request for Post Award Action does NOT constitute an authorization to start work. A Request for Post Award action may include, but not limited to cost and no cost changes, period of performance extensions, within scope changes, shipping or inspections changes.

9.5.2 **Revised TEP for Post Award Actions**

Within seven work days of receipt of the Request for Post Award Action, the Contractor shall submit a Revised TEP, in accordance with the format defined in Section 9.3.2.

9.5.3 **Post Award Action Approval**

The goal is to approve each Revised TEP within five work days of receipt. The Government shall either approve the TEP or enter discussions as soon as practical after TEP receipt. When requested, the Contractor shall provide an updated TEP to address the results of such discussions.

9.6 **REPORTING AND MEETING REQUIREMENTS**

9.6.1 **Reporting Requirements**

The deliverables defined below are required for the basic contract and each resulting TO, unless otherwise specified, and shall be forwarded electronically to the Government. The basic contract report shall be a rollup of each TO. Each individual TO report shall be delivered to the COR for that TO. Any differences between the requirements for the overall basic contract report versus the TO report are noted below.

Each deliverable shall be submitted as set forth in each subparagraph below and shall be Section 508 compliant (for additional information concerning 508 Compliance see Addendum A3.0). Deliverables below will be accepted based in part on satisfaction of the identified Section 508 standards' requirements for accessibility. For monthly reports, the reporting period shall be from the first day of each month (or the date of TO award) through the last day of that month; each deliverable for that period shall then be submitted by the 15th day of each the following months. Deliverables with due dates falling on a weekend or holiday shall be submitted the following Government work day after the weekend or holiday.

9.6.1.1 **Monthly Progress Report**

The Contractor shall submit a Monthly Progress Report for each TO awarded. These reports shall convey the status of the TO performance. TOs that are completed shall be listed as such. A standard format will be provided by VA, and shall be utilized for submission of the below required information. The TO report shall be unique to that TO only.

A For Each TO, indicate/discuss:

1. TO summary
2. Performance metrics
3. TO schedule
4. Major Program VIP Compliance (as applicable)
5. Critical items for Government review
6. Accomplishments
7. An itemized listing of all Information Communication Technology (ICT) deliverables and their current Section 508 conformance status
8. Significant open issues, risk and mitigation action
9. Summary of issues closed
10. Meetings completed
11. Projected meetings
12. Subcontractor performance – discuss first tier Subcontractor(s) performance
13. Projected activities for next reporting period
14. Explanation if the reporting period is over one month
15. Invoice/receiving report submitted
16. Milestone payment schedule
17. Automated bill of materials in data base format

B. General and Cumulative Performance. Indicate the following:

1. Any general meetings that occurred with Government representatives during the reporting period
2. Total dollars awarded to date (ceiling)
3. Total dollars invoiced to date, by fiscal year, and since contract award

C. Performance Metrics

1. Schedule Performance to Plan

The Contractor shall provide a Monthly Progress Report at the basic contract level that provides a roll up of each TO.

9.6.1.2 **Status of Government Furnished Equipment (GFE) Report**

The Contractor shall submit a Monthly Status of GFE Report for each TO. This TO report shall be unique to each TO.

A. TO Number
B. Project Name
C. Employee Name
D. Type of Equipment
E. Tracking Number
F. VA Bar Code
G. Location
H. Value
I. Total Number of Pieces
J. Total Value of Equipment
K. Anticipated Transfer Date to Government
L. Anticipated Transfer Location

The Contractor shall provide a Monthly Status of GFE Report at the basic contract level that provides a roll up of each TO.

9.6.1.3 **Personnel Contractor Manpower Report**

The Contractor shall provide a Monthly Personnel Contractor Manpower Report in MS Excel, listing all personnel for each TO. This report shall be provided at the basic contract level only. The report shall include a separate tab for each TO. The information contained on each tab shall be unique to the individual TO. The information required is as follows:

A. TO Number
B. Employee Name
C. Background Investigation/Clearance level and/or Status
D. Company name
E. Prime/Subcontractor
F. Labor Category
G. Facility location
H. Universal Unique Identifier UUID (Badge Number bottom right of back of badge)
I. Facility where badge was issued
J. Badge Expiration Date
K. Project supporting
L. Tour of Duty Schedule

M. Date Disassociated From Contract (for employees who no longer support this contract)
N. Date Badge Returned to TO COR
O. Contractor Rules of Behavior
P. VA Cyber Security Awareness and Rules of Behavior Training
Q. Annual VA Privacy Training

9.6.1.4 **Contractor Staff Roster**

The Contractor shall provide a Contractor Staff Roster, in accordance with the ProPath (PAL) template (https://www.va.gov/PROPATH/Templates.asp), of Contractor and Subcontractor employees within thirty business days after initial TO award. The Contractor Staff Roster shall be provided at the TO level only. The Contractor Staff Roster shall identify all personnel employed under each TO to begin their background investigations. As personnel changes occur a revised roster is required. The Contractor Staff Roster shall be updated and delivered only to the applicable TO's COR within five days of any changes in employee status, training certification completion status, Background Investigation level status, additions/removal of employees, etc., throughout the PoP. The Contractor Staff Roster shall remain a historical document indicating all past information and which employees are active or inactive. For inactive employees, the roster should indicate the date the employee was separated from the TO and their credentials returned to the TO COR.

The Contractor Staff Roster shall contain:

A. Contractor's Full Name
B. Email Address
C. Place of Birth
D. Date of Birth
E. Security/Privacy Training Completion Dates
F. Risk Designation-individual background investigation level requirement (Refer to Section 4.6 of the TO PWS for investigative requirements by task)
G. Existing Background Investigation and/or Clearance (if applicable)
H. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the TO COR. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.

9.6.1.5 **Small Business Participation Report**

The Contractor shall submit the Small Business Participation Report, using the VA-provided template, on a quarterly basis. The Small Business Participation Report shall be provided at the basic contract level only.

9.6.1.6 **Major Subcontractors**

The VA anticipates that Contractor may engage subcontractors to help support the performance under each task order. The Government defines a Major Subcontractor as any subcontractor that is performing a critical function on any task order. Give the importance of these Major Subcontractors, the Contractor agrees to provide prior written notice and a transition plan to the Government of any termination or replacement of a Major Subcontractor under a task order.

9.7 **MEETINGS AND REVIEWS**

For successful management and contract surveillance, the following meetings and reviews are required.

9.7.1 **EHRM IDIQ Contract Kickoff**

The Government intends to convene a Post-Award Conference within 30 days after contract award. The CO shall notify the Contractor of a specific date, location and agenda within 10 days after contract award.

9.7.2 **TO Kickoff Meetings**

As required by the designated COR, and CO, a kickoff meeting may be held on the TO level after award. Dates, locations, and agenda shall be specified at least five calendar days prior to the meeting.

9.7.3 **Program Reviews**

At the discretion of the CO, Program Review Meetings shall be conducted by the VA TAC Contract Specialist and/or designated COR. Dates, locations, agenda, and attendance requirements shall be specified by the appropriate Government representative, at least five calendar days prior to the meeting.

9.8 **COMMUNICATIONS**

The Contractor shall adhere to the following regarding the Public Release of Information:

a) VA is the public release approval authority for any Contractor, or associated sub-contractor requests for release of public information related to VA's EHRM program.
b) Public release for purposes of this contract is defined as new, unreleased information in press releases, fact sheets, web/online stories or blogs, speeches and industry presentations to either external audiences or VA internal audiences.

c) The Contractor shall coordinate with and gain approval of VA through the VA EHRM program office before releasing any new public information by the Contractor and/or any sub-contractor associated with the VA EHRM program
d) The Contractor and associated sub-contractors shall follow release of public information protocols and processes as determined by VA (the customer).
e) VA will coordinate, when possible, with the Contractor regarding the VA's public release of information relating to VA's EHRM program that is significant in nature and would likely result in media inquiry.